Firebox® Vclass User Guide

Vcontroller™ 4.0

WatchGuard®

Designing peace of mind™

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

PLEASE NOTE: Some components of the WatchGuard Vclass software incorporate source code covered under the GNU General Public License (GPL). To obtian the source code covered under the GPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program"

means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the

Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Part No: 0150-000

WatchGuard Technologies, Inc.
Firebox Vclass Software
End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This Firebox Vclass Software End-User License Agreement ('AGREEMENT') is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ('WATCHGUARD') for the WATCHGUARD Firebox Vclass software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the 'SOFTWARE PRODUCT'). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.
(B) To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product on which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).
(C) In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;
(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;
(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;
(D) Transfer this license to another party unless
(i) the transfer is permanent,
(ii) the third party recipient agrees to the terms of this AGREEMENT, and
(iii) you do not retain any copies of the SOFTWARE PRODUCT; or
(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF

NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5.United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6.Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7.Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8.Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Contents

CHAPTER 1

Introduction

Welcome to WatchGuard®

The WatchGuard Firebox Vclass series of security appliances brings high speed network security to enterprise-class businesses, remote offices, service providers, and data centers.

In the past, a connected enterprise needed a complex set of tools, systems, and personnel for access control, authentication, virtual private networking, network management, and security analysis. These costly systems were difficult to integrate and not easy to update. The WatchGuard Firebox Vclass appliance combines firewall security, VPN support, and powerful traffic management with Fast Ethernet and Gigabit Ethernet connections. The Vclass security ASIC architecture delivers scalable support up to 20,000 VPN tunnels. An Install Wizard and Device Discovery utility shorten the installation time to minutes. Firebox Vclass security appliances include an intuitive, multi-platform Java®-based GUI management console for flexible and effective centralized management.

WatchGuard Firebox Vclass Components

All Firebox Vclass models are fully IPSec-compliant, with built-in core software and management tools designed to provide consistent network security. Every Firebox Vclass is a system made up of the following components:

- Firebox Vclass appliance
- WatchGuard Vcontroller™—a comprehensive management and monitoring software suite
- LiveSecurity Service—a security-related broadcast service

RapidCore™ hardware ensemble
A well-integrated chip set and memory system powers every Firebox Vclass appliance in its primary duties: protecting your network and efficiently managing legitimate data.

WatchGuard Firebox Vclass Operating System™ (OS)
Every Firebox Vclass security appliance is preinstalled with the latest version of the Firebox Vclass Operating System—which is identified on the packaging by a version number. This operating system includes all the software resources that make the appliance fully functional.

WatchGuard Firebox Vclass administrative client applications
The WatchGuard Vcontroller (or the companion WatchGuard CPM client software) gives you full control of all the customizable operating system parameters, including basic system configurations, security policies, maintenance, and activity logging.

Minimum Requirements for the WatchGuard Vcontroller

This section describes the minimum hardware and software requirements necessary to successfully install, run, and administer the WatchGuard Vcontroller.

Note

For the most current information on Vclass hardware and operating system requirements, see the Readme file on the Firebox Vcontroller CD. In addition, updates are frequently posted on the WatchGuard Web site.

Windows workstation

Operating System
Windows 98/ME/NT 4.0/2000/XP

CPU
Pentium II or later

Processor speed
500 MHz or faster

Memory
64 MB minimum (128 MB is recommended)

Input device
CD-ROM or DVD

Hard disk space
10 MB minimum

Additional space as required for log files

Additional space as required for backup and archive configuration files

Network interface
NICs or embedded network connections

Linux workstation

Operating system
Linux kernel v2.2.12 and glibc v2.1.2-11 or later. The officially supported Linux platform for JRE 1.3.1 is RedHat Linux 6.2. Because of localization issues involving Linux platforms, see the Sun Web site.

CPU
Pentium II or later

Processor speed
500 MHz or faster

Memory
64 MB minimum (128 MB is recommended)

Input device
CD-ROM or DVD

Hard disk space
10 MB minimum

Network interface
NICs or embedded network connections

Sun/Solaris workstation

Operating system
Solaris v2.6 or later

Memory
64 MB minimum (128 MB recommended)

Input device
CD-ROM or DVD

Hard disk space
10 MB minimum

Network interface
NICs or embedded network connections

Software License Keys

Keep track of your license key certificates. Your WatchGuard Firebox Vclass comes with a LiveSecurity Service key that activates your subscription to the LiveSecurity Service. For more information on this service, see “Service and Support” on page 7.

Some features of the WatchGuard Firebox Vclass series of appliances must be licensed for use, and others can be expanded by licensing additional capacity. Licensing increases or extends the Firebox Vclass capability in three ways:

- Adding new functionality through optional products
- Increasing the capacity of a particular feature
- Extending the duration of a limited-term feature or service

High Availability and WatchGuard Mobile User VPN are optional products, and you receive those license keys upon purchase. For more information on optional products, see “WatchGuard Firebox Vclass Appliance Options” on page 5. For more information on increasing the capacity or lengthening the duration of a feature, see the WatchGuard Web site.

For information on adding and managing software licenses, see “Managing Software Licenses” on page 97.

WatchGuard Firebox Vclass Appliance Options

The WatchGuard Firebox Vclass appliance is enhanced by several optional products. For more information on any of these options, see the WatchGuard Web site at www.watchguard.com.

High Availability

WatchGuard High Availability software lets you install a second, standby Firebox on your network. If your primary Firebox fails, the second Firebox automatically takes over to give your customers, business partners, and employees virtually uninterrupted access to your protected network.

Mobile User VPN

Mobile User VPN is the WatchGuard IPSec implementation of remote user virtual private networking. Mobile User VPN connects an employee on the road or working from home to the trusted and optional networks behind a Firebox Vclass using a standard Internet connection, without compromising security. VPN traffic is encrypted using DES or 3DES.

About This Guide

The purpose of this guide is to help users of the WatchGuard Firebox Vclass appliance set up and configure a basic network security system and maintain, administer, and enhance the configuration of their network security.

The audience for this guide represents a wide range of experience and expertise in network management and security. The end user of the WatchGuard Firebox Vclass is generally a network administrator for a large enterprise with multiple offices around the world.

The following conventions are used in this guide:

- Within procedures, visual elements of the user interface, such as buttons, drop list items, dialog boxes, fields, and tabs, appear in **boldface**.
- Drop list items separated by arrows (⇒) are selected in sequence from subsequent drop lists. For example, **File** ⇒**Open** ⇒ **Configuration File** means to select **Open** from the **File** drop list, and then **Configuration File** from the **Open** drop list.
- URLs and email addresses appear in sans serif font; for example, wg-users@watchguard.com.
- Code, messages, and file names appear in monospace font; for example:`.wgl` and `.idx` files
- In command syntax, variables appear in italics; for example: fbidsmate *import_passphrase*
- Optional command parameters appear in square brackets.

CHAPTER 2

Service and Support

No Internet security solution is complete without systematic updates and security intelligence. From the latest hacker techniques to the most recently discovered operating system bug, the daily barrage of new threats poses a perpetual challenge to any network security solution. LiveSecurity® Service keeps your security system up-to-date by providing solutions directly to you.

In addition, the WatchGuard Technical Support team and Training department offer a wide variety of methods to answer your questions and assist you with improving the security of your network.

Benefits of LiveSecurity® Service

As the frequency of new attacks and security advisories continues to surge, the task of ensuring that your network is secure becomes an even greater challenge. The WatchGuard Rapid Response Team, a dedicated group of network security experts, helps absorb this burden by monitoring the Internet security landscape for you in order to identify new threats as they emerge.

Threat alerts and expert advice

After a new threat is identified, you'll receive a LiveSecurity broadcast via an email message from our Rapid Response Team that alerts you to the threat. Each alert includes a complete description of the nature and severity of the threat, the risks it poses, and what steps you should take to make sure your network remains continuously protected.

Easy software updates

Your WatchGuard LiveSecurity Service subscription saves you time by providing the latest software to keep your WatchGuard Firebox Vclass up-to-date. You receive installation wizards and release notes with each software update for easy installation. These ongoing updates ensure that your WatchGuard Firebox Vclass remains state-of-the-art, without your having to take time to track new releases.

Access to technical support and training

When you have questions about your WatchGuard Firebox Vclass, you can quickly find answers using our extensive online support resources, or by talking directly to one of our support representatives. In addition, you can access WatchGuard courseware online to learn about WatchGuard Vclass features.

LiveSecurity® Broadcasts

The WatchGuard LiveSecurity Rapid Response Team periodically sends broadcasts and software information directly to your desktop via email. Broadcasts are divided into channels to help you immediately recognize and process incoming information.

Information Alert

Information Alerts provide timely analysis of breaking news and current issues in Internet security combined with system configuration recommendations necessary to protect your network.

Threat Response

After a newly discovered threat is identified, the Rapid Response Team transmits an update specifically addressing this threat to make sure your network is protected.

Software Update

You receive functional software enhancements on an ongoing basis that cover your entire WatchGuard Firebox Vclass.

Editorial

Leading security experts join the WatchGuard Rapid Response Team in contributing useful editorials to provide a source of continuing education on this rapidly changing subject.

Foundations

Articles specifically written for novice security administrators, non-technical co-workers, and executives.

Loopback

A monthly index of LiveSecurity Service broadcasts.

Support Flash

These technical tutorials provide tips for managing the WatchGuard Firebox Vclass. Support Flashes supplement other resources such as FAQs and Known Issues on the Technical Support Web site.

Virus Alert

In cooperation with McAfee, WatchGuard issues weekly broadcasts that provide the latest information on new computer viruses.

New from WatchGuard

To keep you abreast of new features, product upgrades, and upcoming programs, WatchGuard first announces their availability to our existing customers.

Activating the LiveSecurity® Service

The LiveSecurity Service can be activated through the activation section of the WatchGuard LiveSecurity Web pages.

To activate the LiveSecurity Service through the Web:

1 Be sure that you have the Firebox Vclass serial number handy. You will need this during the activation process.
   - The Firebox Vclass serial number is displayed in two locations: a small silver sticker on the outside of the shipping box, and a sticker on the back of the Firebox Vclass just below the UPC bar code

2 Using your Web browser, go to:
http:\\www.watchguard.com\activate

NOTE

You must have JavaScript enabled on your browser to be able to activate LiveSecurity Service.

3 Complete the Account Profile page. Move through the fields on the form using either the TAB key or the mouse.
All of the fields are required for successful registration. The profile information helps WatchGuard target information and updates to your needs.

4 Click **Register**.
The Product Selection page appears.

5 Select your product and click **Next**.
The Activation page appears.

6 Verify that your email address is valid. You will receive your activation confirmation mail and all of your LiveSecurity broadcasts at this address.

7 Enter the serial number of your product.

8 Select the language you prefer.

9 Review the EULA and click **Continue**.
The Feature Key page appears.

10 The Feature Key page displays the unique feature key for your unit.

NOTE

To enable VPN 3DES encryption for your unit, you must copy this feature key information into the Vclass Vcontroller software. For information on copying the feature key into the Vcontroller software, see "Importing LiveSecurity Feature Key" on page 11

11 Click **Continue**. The Confirmation Web page appears.

Importing LiveSecurity Feature Key

To import a feature key from the LiveSecurity Service Web site to the Vcontroller software:

1 Launch the Vcontroller software.

2 Click **System Configuration**.

3 Click on the License tab.

4 Click **Add**.
The Import License window appears.

5 Copy the feature key information generated on Feature Key page from the LiveSecurity Service Web site.

NOTE

If you closed the Feature Key page, you can regenerate your Feature Key by logging back into LiveSecurity Service on the WatchGuard Web site at:
https://www3.watchguard.com/archive/login.asp
Once logged into the LiveSecurity Service, you can regenerate your unit's unique Feature Key by selecting **Get Feature Key**.

6 Click **Paste** in the Import License window.

7 Click **Import License** to add the license.

You completed importing the LiveSecurity feature key. Click **Active Features** to check what features are activated.

LiveSecurity® Self Help Tools

Online support services help you get the most out of your WatchGuard products.

NOTE

You must register for LiveSecurity Service before you can access the online support services.

Advanced FAQs (frequently asked questions)
Detailed information about configuration options and interoperability.

Known Issues
Confirmed issues and fixes for current software.

Interactive Support Forum
A moderated Web board about WatchGuard products.

Online Training
Information on product training, certification, and a broad spectrum of publications about network security and WatchGuard products. These courses are designed to guide users through all components of WatchGuard products. These courses are modular in design, allowing you to use them in a manner most suitable to your learning objectives. For more information, go to:
www.watchguard.com/training/courses_online.asp

Learn About
A listing of all resources available for specific products and features.

Product Documentation
A listing of current product documentation from which you can open.pdf files.

To access the online support services:

1 From your Web browser, go to http://www.watchguard.com/ and select **Support**.

2 Log in to LiveSecurity Service.

Interactive Support Forum

The WatchGuard Interactive Support forum is an online group in which the users of the WatchGuard Firebox Vclass and Firebox System exchange ideas, questions, and tips regarding all aspects of the product, including configuration, compatibility, and networking. This forum is categorized and searchable, and is moderated, during regular business hours, by

WatchGuard engineers and Technical Support personnel. However, this forum should not be used for reporting support issues to WatchGuard Technical Support. Instead, contact WatchGuard Technical Support directly via the Web interface or telephone.

Joining the WatchGuard users forum

To join the WatchGuard users forum:

1 Go to www.watchguard.com. Click **Support**. Log into LiveSecurity Service.

2 Under **Self-Help Tools**, click **Interactive Support Forum**.

3 Click **Create a user forum account**.

4 Enter the required information in the form. Click **Create**.
The username and password should be of your own choosing. They should not be the same as that of your LiveSecurity Service.

5 When you are done, click anywhere outside the box to dismiss it.

Product Documentation

WatchGuard products are fully documented on our Web site at: http://help.watchguard.com/documentation/default.asp.

Assisted Support

WatchGuard offers a variety of technical support services for your WatchGuard products. Several support programs, described throughout this section, are available through WatchGuard Technical Support. For a summary of the current technical support services offered, please refer to the WatchGuard Web site at:

http://support.watchguard.com/aboutsupport.asp

NOTE

You must register for LiveSecurity Service before you can receive technical support.

LiveSecurity® Program

WatchGuard LiveSecurity Technical Support is included with every new Firebox Vclass. This support program is designed to assist you in maintaining your enterprise security system involving our Firebox Vclass, Firebox System, SOHO, ServerLock, AppLock, and VPN products.

Hours

WatchGuard LiveSecurity Technical Support business hours are 4:00 AM to 7:00 PM PST (GMT - 7), Monday through Friday. (Exception: SOHO Program is 24 hours a day, 7 days a week.)

Phone Contact

877.232.3531 in U.S. and Canada
+1.360.482.1083 all other countries

Web Contact

http://www.watchguard.com/support

Response Time

Four (4) business hours maximum target

Type of Service

Technical assistance for specific issues concerning the installation and ongoing maintenance of Firebox Vclass, Firebox System, SOHO, and ServerLock enterprise systems

Single Incident Priority Response Upgrade (SIPRU) and Single Incident After-hours Upgrade (SIAU) are available. For more information, please refer to WatchGuard Web site at:

http://support.watchguard.com/lssupport.asp

LiveSecurity® Gold Program

This premium program is designed to meet the aggressive support needs of companies that are heavily dependent upon the Internet for Web-based commerce or VPN tunnels.

WatchGuard Gold LiveSecurity Technical Support offers support coverage 24 hours a day, seven days a week. Our Priority Support Team is available continuously from 7 PM Sunday to 7 PM Friday Pacific Time (GMT – 7), and can help you with any technical issues you might have during these hours.

We target a one-hour maximum response time for all new incoming cases. If a technician is not immediately available to help you, a support administrator will log your call in our case response system and issue a support incident number.

Firebox Vclass Installation Services

WatchGuard Remote Firebox Vclass Installation Services are designed to provide you with comprehensive assistance for basic Firebox Vclass installation. You can schedule a dedicated two-hour time slot with one of our WatchGuard technicians to help you review your network and security policy, install the LiveSecurity software and Firebox Vclass hardware, and build a configuration in accordance with your company security policy. VPN setup is not included as part of this service.

VPN Installation Services

WatchGuard Remote VPN Installation Services are designed to provide you with comprehensive assistance for basic VPN installation. You can schedule a dedicated two-hour time slot with one of our WatchGuard technicians to review your VPN policy, help you configure your VPN tunnels, and test your VPN configuration. This service assumes you have already properly installed and configured your Firebox Vclass appliances.

Training and Certification

WatchGuard offers training, certification, and a broad spectrum of publications to customers and partners who want to learn more about network security and WatchGuard products. No matter where you are located or which products you own, we have a training solution for you.

WatchGuard classroom training is available worldwide through an extensive network of WatchGuard Certified Training Partners (WCTPs). WCTPs strengthen our relationships with our partners and customers by providing top-notch instructor-led training in a local setting.

WatchGuard offers product and sales certification, focusing on acknowledging the skills necessary to configure, deploy and manage enterprise security solutions.

Using the Online Help

Online help is available from almost all WatchGuard Vcontroller windows. Because the online help uses Web browsers for display, you should be aware of a problem in opening help in Netscape browsers. If you use a Netscape browser on a workstation running any Microsoft Windows operating system, version 4.7.3 or later is required for online help to work properly.

CHAPTER 3

Getting Started

The Firebox Vclass appliance acts as a barrier between your networks and the public Internet, protecting them from security threats. This chapter explains how to install the Firebox Vclass appliance into your network. You must complete the following steps in the installation process:

- "Gathering Network Information" on page 18
- "Setting up the Management Station" on page 18
- "Cabling the Appliance" on page 22
- "Turning on a Firebox Vclass Security Appliance" on page 22
- "Using Appliance Discovery" on page 23
- "Running the Vcontroller Installation Wizard" on page 27
- "Deploying the Firebox Vclass into your Network" on page 43

For a quick summary of this information, see the WatchGuard Firebox Vclass *QuickStart Guide* included with your Firebox Vclass appliance.

This chapter is intended for new WatchGuard Firebox Vclass installations only. If you have a previously installed appliance with a prior software version, connect to it with Vcontroller, and then follow the upgrade instructions as described in "Upgrading and Downgrading the Software Version" on page 57.

If you already have one or more operational Firebox Vclass appliances in your network with the current software version, you can shortcut the installation and configuration process on a new factory-default appliance. For more information, see “Importing a Profile into a New Appliance” on page 55.

Before installing the Firebox Vclass appliance, verify the package contents. Consult the *Firebox Vclass Hardware Guide* to make sure you have received all of the proper contents.

Gathering Network Information

One good way to set up your network is to create two worksheets: the first worksheet represents your network now—before deploying the Firebox Vclass appliance—and the second represents your network after the Firebox Vclass appliance is deployed.

Setting up the Management Station

The Management Station runs the Vcontroller software, which is the primary administrative access to the appliance. The Management Station can also be used to archive log messages generated by the Log Manager. For more information on the Log Manager, see “Using Log Manager” on page 243.

You can designate any computer or computers on your network as Management Stations.

Installing the Vcontroller on a Windows workstation

Before you install the Vcontroller software, make sure you have gathered all of the network addressing information that represents your new Firebox Vclass security appliance. Use the worksheet you filled out in the previous section, “Gathering Network Information” on page 18.

NOTE

Review the release notes included with this package for information about Windows-Java issues, including the Windows and JRE versions. For additional updates, check the WatchGuard Web site.

To install Vcontroller, follow these steps:

1. Remove the Vcontroller CD from the package and insert it in the workstation CD-ROM.
2. Locate and double-click the CD-ROM drive icon (usually found in the My Computer window). If AutoRun is enabled on the CD drive, the Installer launches automatically.
3. When the CD window contents appear, double-click the Windows folder.
4. When that window’s contents appear, double-click the **setup.exe** icon to start the installation of the Vcontroller software.
5. The installer may detect older versions of the Java Run-time Environment (JRE) and the Java Development Kit (JDK) or a version it cannot verify. WatchGuard recommends installing the version included on your CD over any existing versions.
6. When the process is finished, a window appears, prompting you to start Vcontroller.

Installing the Vcontroller on a Solaris workstation

Before you install the Vcontroller software, make sure you have gathered all of the network addressing information that will represent your new Firebox Vclass security appliance. Use the worksheet you filled out in the previous section, “Gathering Network Information” on page 18.

NOTE

Be sure to review the release notes that were included in this package for information about Solaris-Java issues, including the Solaris and JRE versions. For additional updates, check the WatchGuard Web site.

To install the Vcontroller, follow these steps:

1 Insert the WatchGuard CD into the CD-ROM. (Under Solaris, the CD should automatically mount at /cdrom).

2 Execute the installer application by entering the following commands:

```
cd /cdrom/watchguard
./setup.sh
```

3 The installer asks whether you have already installed the latest versions of the Java Run-time Environment (JRE) and JDK. If you have, type **Y** and then type the pathways of the JRE and JDK directories.

NOTE

If you have an older version of JDK, the installer asks whether you prefer to use it instead of a more recent version. WatchGuard recommends that you install the most recent version.

4 If you have not installed JRE or JDK, type **N**. The installer quits, but provides information on where to obtain the most current versions of JRE and JDK software from the Sun Web site.

5 When the JRE and JDK software have been installed and any required Solaris updates are completed, execute the installer application again by entering the following commands:

```
cd /cdrom/watchguard
./setup.sh
```

6 When asked by the installation script for the directory location of the JRE and JDK software, enter the appropriate pathway.

7 Vcontroller installation is complete. To launch Vcontroller execute the following command: `Vcontroller`

Be certain the directory containing the Vcontroller software is listed in the PATH environment variable.

Installing the Vcontroller on a Linux workstation

Before proceeding with the following, make sure you have all of the network addressing information that represents your new Firebox Vclass security appliance. Use the worksheet you filled out in the previous section, "Gathering Network Information" on page 18.

NOTE

Be sure to review the release notes that were included in this package for information about Linux-Java issues, including the Linux and JRE versions. For additional updates, check the WatchGuard Web site.

To install the Vcontroller, follow these steps:

1 Insert the WatchGuard CD into the CD-ROM.

2 Execute the installer application by entering the following commands:

```
mount /dev/cdrom -t iso9660 /mnt/cdrom
cd /mnt/cdrom
./setup.sh
```

3 The installer asks whether you have already installed the latest versions of the Java Run-time Environment (JRE) and JDK. If you have, type **Y** and then type the pathways of the JRE and JDK directories.

NOTE

If you have an older version of JDK, the installer asks whether you prefer to use it instead of a more recent version. WatchGuard recommends that you install the most recent version.

4 If you have not installed JRE or JDK, type **N**. The installer quits, but provides information on where to obtain the most current versions of JRE and JDK software from the Sun Web site.

5 When the JRE and JDK software has been installed and any required Linux updates are completed, execute the installer application again by entering the following commands:

```
cd /cdrom/watchguard
./setup.sh
```

6 When asked by the installation script for the directory location of the JRE and JDK, enter the appropriate pathway.

7 Vcontroller installation is complete. To launch Vcontroller execute the following command: `Vcontroller`

Be certain the directory containing the Vcontroller software is listed in the PATH environment variable.

NOTE

Some versions of the JRE and JDK for Linux may display fonts incorrectly. In addition, you may encounter a "font not found" error.

Cabling the Appliance

The next procedure in the installation process is cabling the appliance to the Management Station. Refer to the *Firebox Vclass Hardware Guide* to make sure you have received all of the necessary cables.

1 Remove the Firebox Vclass appliance from its packaging.

2 Place the appliance on any stable flat surface near the Management Station.

3 Connect the appliance through interface **0** (Private) to the Management Station using the red crossover Ethernet cable (or corresponding optical cable depending upon the Firebox model).

4 Connect the appliance to a nearby power source using the power cord. If connecting the appliance to a UPS device, be sure to use the WatchGuard-supplied cable to connect the two devices through their respective RS-232 ports.

Turning on a Firebox Vclass Security Appliance

After you have placed the appliance on a surface near the Management Station and have made the network connections, you can power up the Firebox Vclass appliance. The following instructions are for all models except the Firebox V10. After you have plugged in the appliance, turn the appliance on using the switch on the back. The Ready LED will blink while the appliance initializes itself. When the appliance is ready, the light will stop blinking and remain solidly lit. This may take two or three minutes.

When the appliance has been fully powered up and initialized, the following lights on the front of the device should be lit:

- The Power LED
- The Ready LED
- One of the Private, Public, and DMZ interface speed indicator lights, if those connections have been made.

If problems occur

If the expected indicators are not active, check the following:

- If the Power LED is not lit, disconnect and reconnect the power cord.
- If the Ready LED is still blinking after more than five minutes, use the power switch on the back of the appliance to cut the power, and then restore power and reinitiate the startup process.
- Make sure all data cables and the power cord are fully seated in their sockets.

Using Appliance Discovery

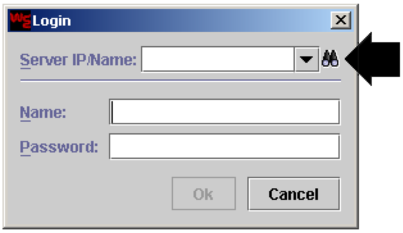
After the WatchGuard Vcontroller is installed on the Management Station, you can use Vcontroller to discover any new factory default appliance on the network.

This appliance *must* be connected to the same LAN segment or subnet as the Management Station through interface **0** (Private).

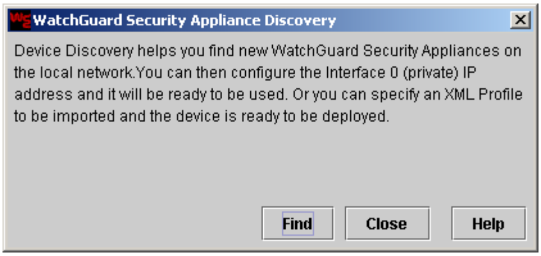
1 Launch Vcontroller.

The Vcontroller and Login dialog boxes appear.

2 Click the binoculars icon to the right of the **Server/IP Name** drop list.



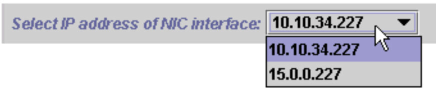
The WatchGuard Security Appliance Discovery dialog box appears.



Device Discovery helps you find new WatchGuard Security Appliances on the local network.You can then configure the Interface 0 (private) IP address and it will be ready to be used. Or you can specify an XML Profile to be imported and the device is ready to be deployed.

3 Click **Find** to start the process.

If the Management Station has more than one NIC, you *must* select the IP address of the appropriate card from the drop list before proceeding.



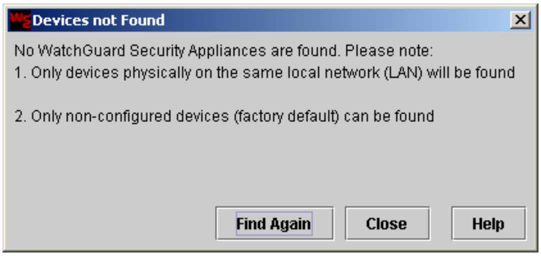
Select IP address of NIC interface: 10.10.34.227

A status dialog box appears and remains open until the discovery process is complete.

Searching ...

If no appliance is discovered

If no appliances are discovered, a **Devices Not Found** dialog box appears.



No WatchGuard Security Appliances are found. Please note:
1. Only devices physically on the same local network (LAN) will be found

2. Only non-configured devices (factory default) can be found

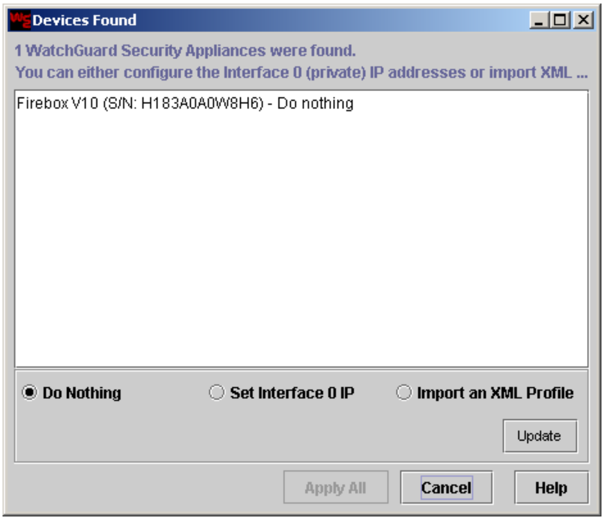
Check the Firebox Vclass appliance for the following:

- Verify that the appliance has been properly connected to the network.
- Verify that all cable connections are secure.
- Make sure that the appliance has fully powered up. The Ready LED should be steadily lit.

Click **Find Again** to attempt another discovery.

If an appliance is discovered

When an appliance is discovered, the **Devices Found** dialog box appears, displaying all discovered appliances with their models and serial numbers.



1 WatchGuard Security Appliances were found.
You can either configure the Interface 0 (private) IP addresses or import XML ...

Firebox V10 (S/N: H183A0A0W8H6) - Do nothing

● Do Nothing ○ Set Interface 0 IP ○ Import an XML Profile

This window provides the following features:

- A large list area that displays all of the appliances discovered in the local subnet. In this case, only your new Firebox Vclass appliance will be listed. You can set interface **0** (Private) IP addresses or import profiles into more than one appliance at the same time.
- A collection of options that enable you to set the identity of a selected appliance’s Private interface or import an existing appliance profile into a selected device.

You set the IP address of the Interface 0 as described in the following section. This is the task you perform with a new appliance.

NOTE

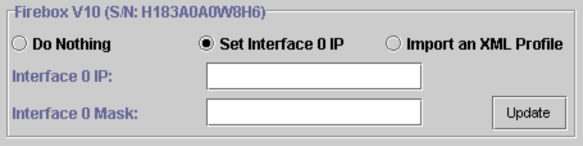
If you have already installed and configured at least one Firebox Vclass appliance, you can import its configurations into a new factory default appliance using an XML-format profile. For more information, see "Exporting and Importing Configuration Files" on page 267.

Setting the IP address of Interface 0 (Private)

You must now define a temporary IP address to interface 0 (Private) for use in the initial configuration. After this is complete, you can log in with Vcontroller and perform further configuration.

1 From the **Devices Found** field, select the appliance you want to configure.

2 Click the **Set Interface 0 IP** button.



Firebox V10 (S/N: H183A0A0W8H6)

○ Do Nothing ● Set Interface 0 IP ○ Import an XML Profile

Interface 0 IP:

Interface 0 Mask:

3 In the **Interface 0 IP** field, type an unused IP address from the same subnet as the Management Station.

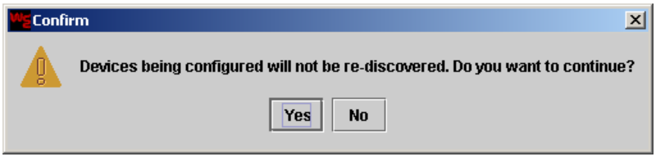
4 In the **Interface 0 Mask** field, type the subnet mask for this IP address.

5 Click **Update**.

If more than one appliance is listed in this window, you can set an IP address for each appliance at this time, prior to clicking Apply All.

6 If there are no more appliances to be set, click **Apply All**.

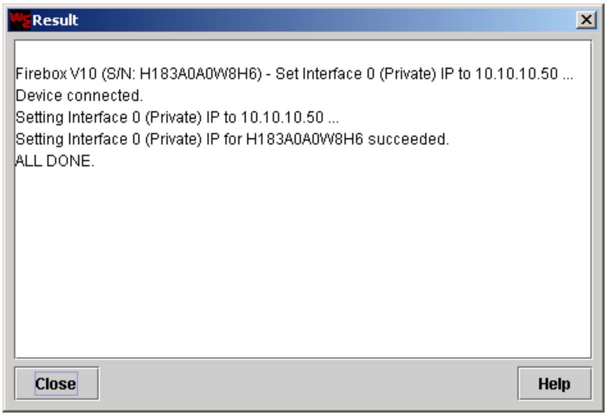
A confirmation window appears.



Confirm

Devices being configured will not be re-discovered. Do you want to continue?

7 Click **Yes** to proceed.
The Result window appears.



```
Firebox V10 (S/N: H183A0A0W8H6) - Set Interface 0 (Private) IP to 10.10.10.50 ...
Device connected.
Setting Interface 0 (Private) IP to 10.10.10.50 ...
Setting Interface 0 (Private) IP for H183A0A0W8H6 succeeded.
ALL DONE.
```

8 Wait for the Result window to display “ALL DONE” and then click **Close** to restart the appliance and return to the Set Interface window.
The appliance will restart; restarting lasts a minute or two.

9 After restarting is complete, click **Cancel** to close the Devices Found window.

You can now use the Vcontroller Login window to log into this appliance using the newly assigned IP address and continue the installation process.

Running the Vcontroller Installation Wizard

This section guides you through the *Installation Wizard*, a component of the Vcontroller application. The Installation Wizard provides the basic configuration for a new appliance and prepares the Vcontroller software for use with this and other Firebox Vclass appliances.

Before You Begin

To complete the initial installation of a new Firebox Vclass appliance, you need the following network address information:

- The IP addresses and network masks to assign to the interfaces of this appliance

- A domain name for this appliance
- Any basic network routing information (static and dynamic)
- The IP addresses of all DNS servers that will be used by this appliance
- The IP addresses of any SNMP management stations
- The VPN client user name and password (for Firebox V10 setup)

If you need to make any changes to the configuration at a later date, you can do so with the **System Configuration** dialog box, as described in "System Configuration" on page 61.

Starting the Installation Wizard

1 Power up the Firebox Vclass appliance.

2 Launch Vcontroller and click **Login**.
The Login dialog box appears.

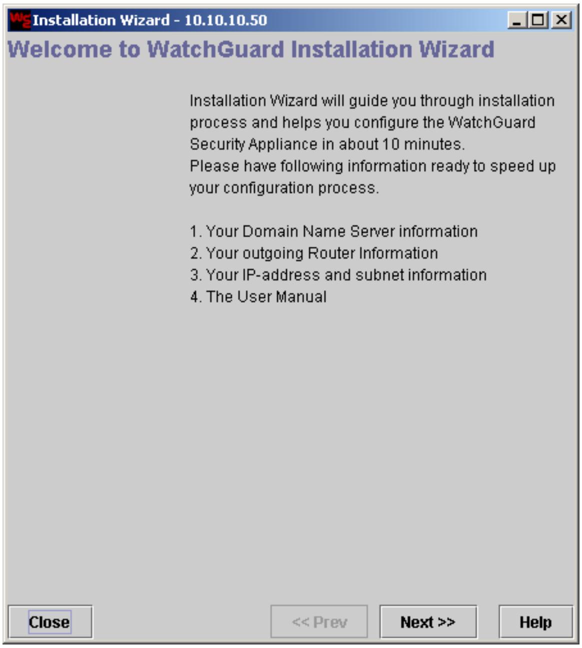
3 Type the IP address or host name of the Firebox Vclass in the Server **IP/Name** field or select it from the drop list.

4 Type your administrator login name and password in the appropriate fields. The default name and password for the Firebox Vclass appliance is admin.

NOTE

All data traffic between the Management Station and the Firebox Vclass appliance, including all configuration exchanges, is protected by SSL, using 128-bit RC4 and SHA1.

5 Click **OK**.
The Installation Wizard Welcome screen appears.



Welcome to WatchGuard Installation Wizard

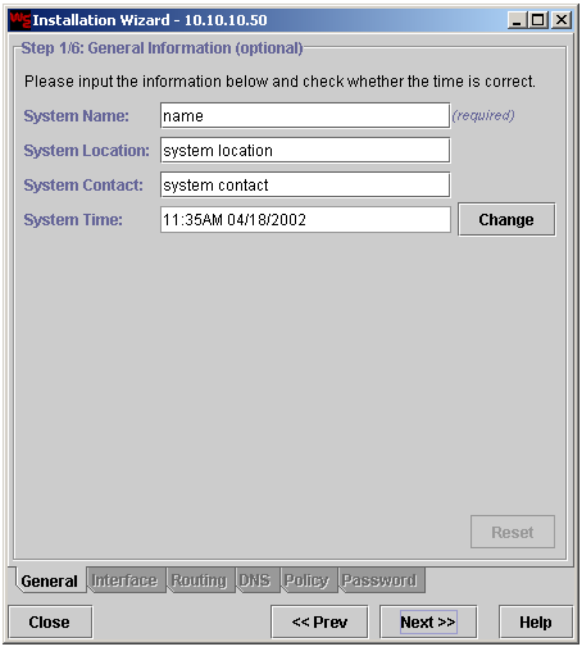
Installation Wizard will guide you through installation process and helps you configure the WatchGuard Security Appliance in about 10 minutes.
Please have following information ready to speed up your configuration process.

1. Your Domain Name Server information
2. Your outgoing Router Information
3. Your IP-address and subnet information
4. The User Manual

6 Read the qualifications and instructions.

Edit the General information

1 Click **Next** to proceed.
The General Information screen appears.



Installation Wizard - 10.10.10.50

Step 1/6: General Information (optional)

Please input the information below and check whether the time is correct.

System Name: name (required)

System Location: system location

System Contact: system contact

System Time: 11:35AM 04/18/2002

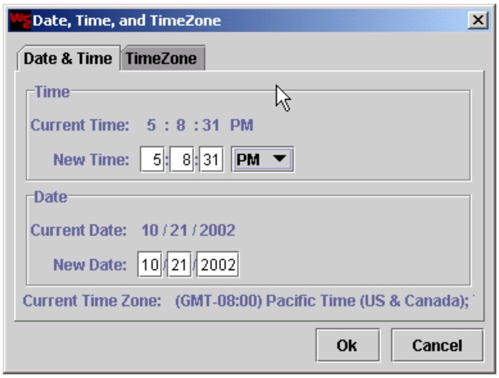
2 In the **System Name** field, type either the assigned DNS name for the appliance or another arbitrary name.

3 In the **System Location** field, type a description of where your appliance will be used. This can be a building, floor number, office name, or other simple description.

4 In the **System Contact** field, enter the name and phone number or email address of the principal administrator or department responsible for management of the appliance.

Changing the System Time, Date and Time Zone

Click **Change** to open the Date, Time, and Time Zone window. Make any necessary adjustments, and click **OK**.



Time

Current Time: 5 : 8 :31 PM

New Time: 5 : 8 : 31 PM

Date

Current Date: 10 / 21 / 2002

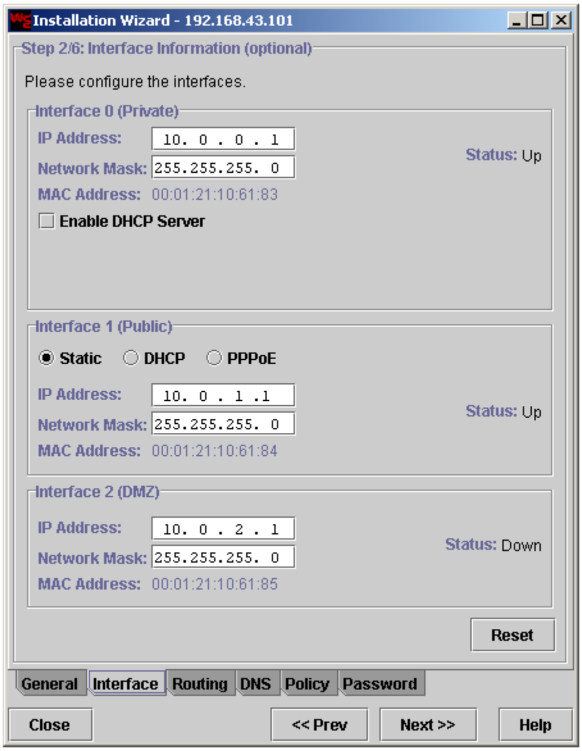
New Date: 10 / 21 / 2002

Current Time Zone: (GMT-08:00) Pacific Time (US & Canada);

Configure the Interfaces

1 Click **Next**.

The Interface Information screen appears.



Installation Wizard - 192.168.43.101

Step 2/6: Interface Information (optional)

Please configure the interfaces.

Interface 0 (Private)

IP Address: 10. 0 . 0 . 1

Network Mask: 255.255.255. 0

MAC Address: 00:01:21:10:61:83

Status: Up

□ Enable DHCP Server

Interface 1 (Public)

● Static ○ DHCP ○ PPPoE

IP Address: 10. 0 . 1 .1

Network Mask: 255.255.255. 0

MAC Address: 00:01:21:10:61:84

Status: Up

Interface 2 (DMZ)

IP Address: 10. 0 . 2 . 1

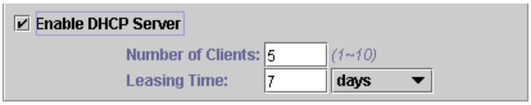
Network Mask: 255.255.255. 0

MAC Address: 00:01:21:10:61:85

Status: Down

2 Enter the IP address and network mask for interface 0 (Private) in the appropriate fields.

3 If you want to enable the appliance as a DHCP server, click **Enable DHCP Server**.



☑ Enable DHCP Server

Number of Clients: 5 (1~10)

Leasing Time: 7 days

4 Enter the maximum number of potential clients that will be assigned IP addresses in the **Number of Clients** field.

5 Select either **Days** or **Hours** from the **Leasing Time** drop list.

6 Type the number of hours or days that an IP address will be loaned to a DHCP client.

7 To configure Interface 1 (Public) for Static, DHCP, or PPPoE addressing, enable the appropriate interface option and provide the relevant entries as follows:

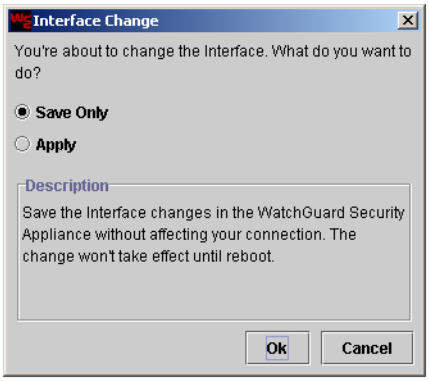
Static IP
Enter the IP address and network mask in the appropriate fields.

DHCP
Enter the IP address or DNS host name of the DHCP server assigned by your ISP in the Host ID field. (This entry is optional.)

PPPoE
Enter the user name and password assigned to you by your ISP in the appropriate fields.

8 To configure Interface 2 (DMZ), enter the IP address and network mask in the appropriate fields.

9 When you have finished with the Interface screen entries, click **Next**.
The Interface Change dialog box appears providing two options, Save Only and Apply.


Interface Change

You're about to change the Interface. What do you want to do?

● Save Only

○ Apply

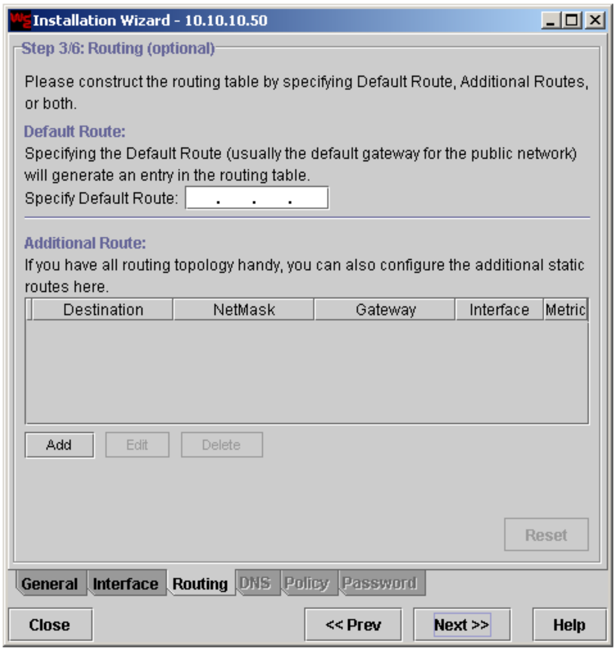
Description

Save the Interface changes in the WatchGuard Security Appliance without affecting your connection. The change won't take effect until reboot.

10 Select **Save Only**. Click **OK** to proceed.
WatchGuard recommends selecting Save Only in order to continue with the Installation Wizard.
If you select **Apply**, and then click **OK,** the Wizard prompts you to stop the installation process and restart the Firebox Vclass appliance to apply the changes. You will need to login again, using the new IP address information, to continue configuring the appliance. For information on configuring the appliance without using the Installation Wizard, see “System Configuration” on page 61.

Configure Routing

1 From the Interface Information window, click **Next**.
The Routing screen appears.


Installation Wizard - 10.10.10.50
Step 3/6: Routing (optional)

Please construct the routing table by specifying Default Route, Additional Routes, or both.

Default Route:

Specifying the Default Route (usually the default gateway for the public network) will generate an entry in the routing table.

Specify Default Route: . . .

Additional Route:

If you have all routing topology handy, you can also configure the additional static routes here.

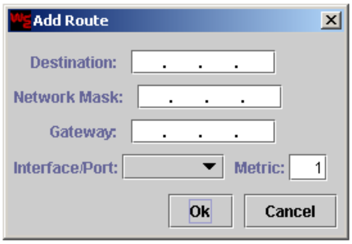
Destination	NetMask	Gateway	Interface	Metric

NOTE

All entries made to configure routing are optional for completing the Installation Wizard and are dependent upon your network environment.

1 Type the IP address of the default gateway in the **Specify Default Route** field.

2 If you want to enter any additional network routes for this appliance, click **Add**.
The Add Route dialog box appears.



3 Type the destination IP address, network mask, and gateway of the route in the appropriate fields.

4 Select the interface—0, 1, or 2—through which traffic will be exchanged, from the **Interface/Port** drop list.

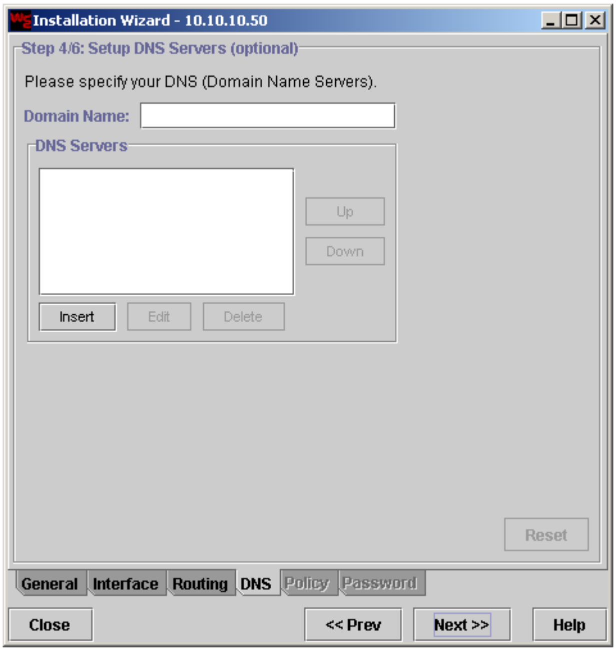
5 Type the Metric number in the appropriate field.

6 Click **OK**.

7 Repeat this process as needed.

Define the DNS servers

1 When you have finished adding routes, click **Next** to proceed to the next step of the Installation Wizard. If you added any new routes, a confirmation window appears, click **OK**.
The Setup DNS Servers screen appears.


Installation Wizard - 10.10.10.50

Step 4/6: Setup DNS Servers (optional)

Please specify your DNS (Domain Name Servers).

Domain Name:

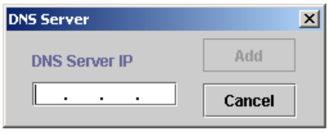
DNS Servers

NOTE

All entries made to configure DNS servers are optional for completing the Installation Wizard, and will differ based on your network configuration.

1 Type the domain name of the Firebox Vclass appliance in the appropriate field.

2 To add a DNS server, click **Insert**.
The DNS Server window appears.


DNS Server

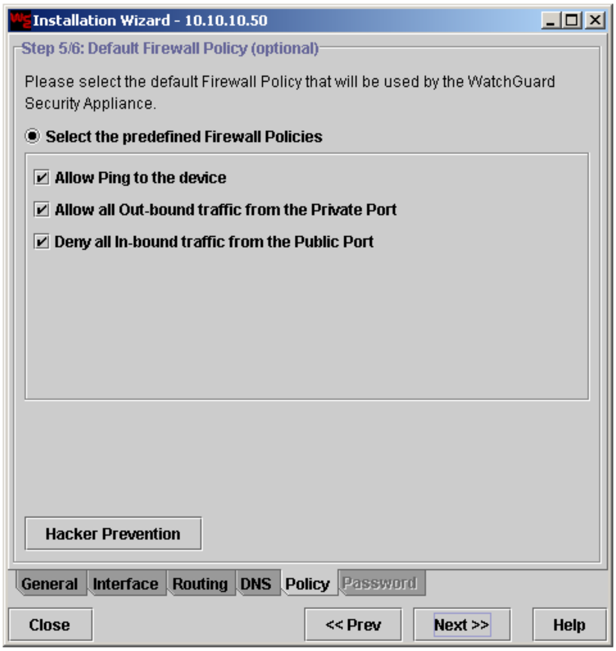
DNS Server IP

3 Type the DNS server IP address in the appropriate field and then click **Add**.
Repeat this process if needed to add more DNS servers.

Define a Default Firewall Policy

1 When you have finished listing the DNS servers, click **Next** to proceed.

The Default Firewall Policy screen appears.



Installation Wizard - 10.10.10.50

Step 5/6: Default Firewall Policy (optional)

Please select the default Firewall Policy that will be used by the WatchGuard Security Appliance.

● Select the predefined Firewall Policies

☑ Allow Ping to the device

☑ Allow all Out-bound traffic from the Private Port

☑ Deny all In-bound traffic from the Public Port

NOTE

All entries made to configure the default firewall policy are optional for completing the Installation Wizard and are dependent upon your network environment.

2 Determine your default firewall policy or select the **No Change** option.

3 If you decide to activate the default firewall policy, click to select the **Select the predefined Firewall Policies** checkbox and then determine which of the following predefined policies you want to enable.

Allow ping to the device

Allows ping traffic to the private interface of this appliance from other workstations within the network.

Allow all Out-bound traffic from the Private Port

Allows all internal network users to have unlimited access to all external network connections.

Deny all In-bound traffic from the Public Port

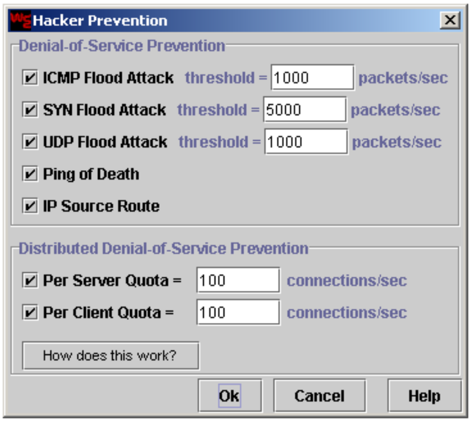
Blocks all incoming traffic from external networks to Interface 1 (Public). If you want to permit particular types of traffic to gain access to part or all of your network, activate the relevant policy. You can later customize your firewall policies to provide further protections. For more information on configuring firewall policies, see “About Security Policies” on page 113.

NOTE

If you do not activate any predefined policy, you must configure a customized security policy. Otherwise, the Firebox Vclass appliance will not permit any traffic to pass through in any direction.

4 To enable a variety of measures to counteract hackers, click the **Hacker Prevention** button at the bottom of the screen.

The Hacker Prevention dialog box appears.



Hacker Prevention

Denial-of-Service Prevention

☑ ICMP Flood Attack threshold = 1000 packets/sec

☑ SYN Flood Attack threshold = 5000 packets/sec

☑ UDP Flood Attack threshold = 1000 packets/sec

☑ Ping of Death

☑ IP Source Route

Distributed Denial-of-Service Prevention

☑ Per Server Quota = 100 connections/sec

☑ Per Client Quota = 100 connections/sec

Denial of service preventions

These options safeguard your servers from Denial of Service (DoS) attacks. Denial of Service attacks flood your network with requests for information, clogging your servers and possibly shutting down your sites.

ICMP Flood Attack
Protects against a sustained flood of ICMP pings. Enable this option, then type the threshold number in the text field.

SYN Flood Attack
Protects against a sustained flood of TCP SYN requests without the corresponding ACK response. Enable this option, then type the threshold number in the text field.

UDP Flood Attack
Protects against a sustained flood of UDP packets. Enable this option, then type the threshold number in the text field.

Ping of Death
Protects against user-defined large data-packet pings.

IP Source Route
Protects against a flood of false client IP addresses, designed to bypass firewall security.

Distributed denial of service options

As a subset of Denial of Service attacks, Distributed DoS (DDoS) attacks occur when hackers coordinate a number of compromised computers for malicious purposes and program them to simultaneously assault a network with information requests. If this type of attack is allowed to pass through, your servers can be overwhelmed, causing a crash.

Per Server Quota
Safeguards your servers against attacks from any client to any single server. Enable this option, then type the threshold number in the text field. The number here represents the maximum request capacity per second of the server. If more than the specified number of connection requests are received, the Firebox Vclass appliance drops the excess requests.

Per Client Quota

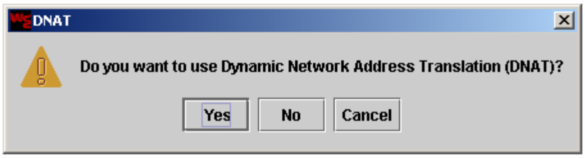
Restricts the number of connection requests from a single client in one second. Enable this option, then type the threshold number in the appropriate text field. This number represents the maximum number of requests per second from a single client. If more than the specified number of connection requests are received, the Firebox Vclass appliance drops the excess requests.

For a brief overview of the distributed denial-of-service options, click **How does this work?** An online Help window displays more information about these options.

Using Dynamic Network Address Translation (DNAT)

1 When you have configured the preferred levels of hacker defense, click **OK** to close this window, and click **Next** to proceed.

If you enabled the Allow all outbound traffic from the Interface 0 (private) option, a DNAT window appears.



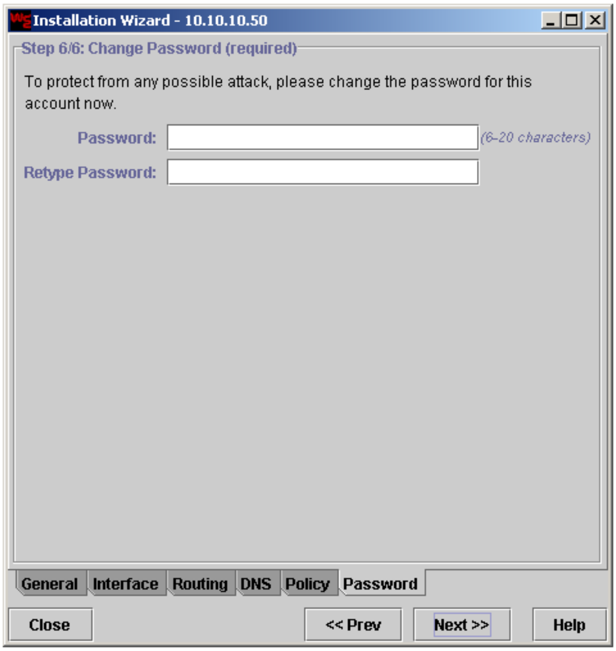
Do you want to use Dynamic Network Address Translation (DNAT)?

2 If you want to use dynamic NAT, click **Yes**.

A default dynamic NAT policy is added to the outbound traffic policy.

Change the Password

The Change Password screen appears. This step requires you to replace the default root admin account password with a new, secure password of your choosing.



Installation Wizard - 10.10.10.50

Step 6/6: Change Password (required)

To protect from any possible attack, please change the password for this account now.

Password: (6-20 characters)

Retype Password:

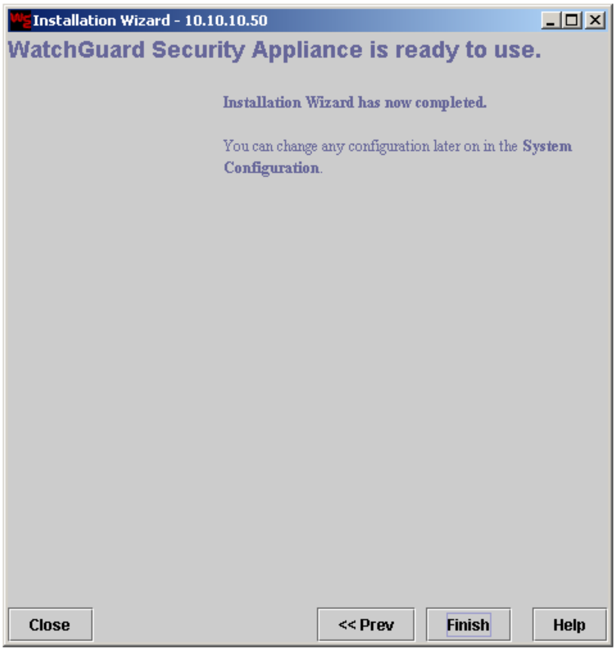
1 Type a new password in the appropriate field.

Passwords must be between 6 and 20 characters, can include letters or numbers, and are case-sensitive.

2 Confirm the password by retyping it in the provided field.

3 When you have finished, click **Next** to proceed.

The completion window appears.


Installation Wizard - 10.10.10.50

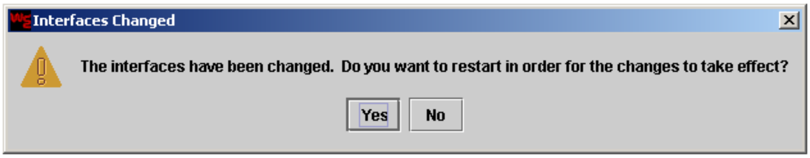
WatchGuard Security Appliance is ready to use.

Installation Wizard has now completed.

You can change any configuration later on in the **System Configuration**.

4 Click **Finish**.

5 If you changed the IP address for interface 0 (Private), a window appears, asking if you want to restart the Firebox Vclass appliance. Click **Yes**.


Interfaces Changed

The interfaces have been changed. Do you want to restart in order for the changes to take effect?

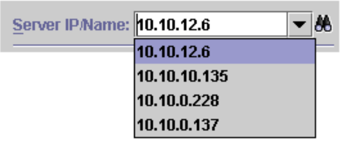
The Firebox Vclass appliance reboots and reinitializes itself.

Deploying the Firebox Vclass into your Network

After the appliance has rebooted, restart the Vcontroller and perform a complete shutdown of the appliance. When the shutdown is complete, you can power down the appliance and move it to a permanent network setting.

1 Launch Vcontroller.

2 Type the IP address of interface 0 (Private) or the host name in the appropriate field.
The Vcontroller remembers the IP addresses of all appliances and stores them in this drop list. You will, however, need to remember all the separate passwords.



3 Type `admin` in the **Name** field.

4 Type your newly created secure password in the **Password** field.

5 Click **OK** to connect to the appliance.
The main Vcontroller window appears.

6 Click **Shut down**.

7 When the shutdown confirmation window appears, click **OK**.
The appliance performs a full shutdown. The Ready LED blinks for a short interval and then turns off when shutdown is complete.

NOTE

Do not power down the appliance until the Power and Ready LEDs have been off for 30 seconds.

8 Turn off the power switch on the back of the appliance, or, for a V10 appliance, disconnect the power cord, to complete the shutdown.

9 Disconnect all the cables and move the appliance to its permanent network setting.

After you place the appliance in its permanent location and make the necessary physical network connections, you can turn it back on.

- Use the power cord to connect the appliance to a UPS device or to a protected outlet. This will power up the V10 appliance.

- Turn on the power switch on the back of the appliance.

  When the appliance has fully powered up, the Ready LED blinks while the initialization process occurs. When initialization is complete, the Ready LED remains lit.

CHAPTER 4

Firebox Vclass Basics

This chapter provides an overview of the Firebox Vclass hardware and the companion Vcontroller software.

What is a Firebox Vclass Appliance?

Every Firebox Vclass appliance is a combination of powerful network-monitoring hardware and software policies that you, the administrator, set up and maintain. With every incoming or outgoing data stream that it detects, the appliance performs a two-stage task:

- It analyzes the initial packet for key traffic specifications, including source, destination, type of service, and specific appliance interface used by the data stream.
- If the data matches all the specifications established in a given policy, the appliance takes action—directing that packet and the stream that follows to the desired destination. It can also block the traffic.

A policy can also prompt the Firebox Vclass appliance to take other actions with the same data stream, as dictated by the policy.

You can create policies for the Firebox Vclass that watch for varying combinations of traffic specifications. After a set of traffic specifications are defined, you can set up one or more actions that the Firebox Vclass appliance should take with any qualifying data.

Firebox Vclass Features

The Firebox appliances provide the following features:

Firewall
Protects your network from unauthorized access and use.

Load balancing (except the V10 model)
Distributes incoming data to specific internal destinations.

Quality of Service
Makes data exchanges more efficient. Prioritizes and enhances user-specified data exchange.

Anti-hacker protection
Protects your network from a variety of potentially destructive hacker attacks.

VPN (Virtual Private Networking)
Provides secure communications with remote sites.

Dynamic NAT (Network Address Translation)
Also called IP Masquerading. Maps outgoing private IP addresses to the Firebox’s external IP address, meaning outgoing source IP addresses are translated into the IP address of the box’s external interface. Incoming packets are translated from the external interface's IP address into the appropriate private IP address.

Static NAT (except the V10 model)
Also called port forwarding. Assigns a port specific to a given service (such as port 80 for HTTP) to another port internally, so that originators of incoming traffic never know which host is actually receiving the packets.

Multi-tenant domains (except the V10 model)
Manages traffic routed to and from both kinds of multiple-tenant virtual domains: user domains and VLANs.

Where the Information is Stored

When you use the Vcontroller to connect to a Firebox Vclass appliance, the Vcontroller accesses a specialized database stored in the Firebox Vclass appliance. This storage capacity is an integral part of the appliance hardware. All your configuration and policy entries are stored in this database.

Certain files, such as backup configuration files, log files, and archive files, can be stored in a location of your choosing, such as the Management Station hard drive or a syslog server.

Changes or additions to the configuration settings in the Vcontroller reside on the Management Station and are not automatically applied to the appliance.

Launching the WatchGuard Vcontroller

The WatchGuard Vcontroller can be used to administer one or more Firebox Vclass appliances as well as any legacy RapidStream security appliances. This Java application offers a basic set of system indicators and three collections of button-activated features that provide complete control over all the operations of a Firebox Vclass appliance.

1 Launch the Vcontroller according to the operating system you are using:

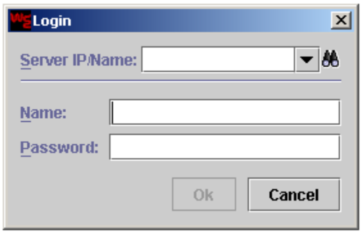
Microsoft Windows

Double-click the WatchGuard Vcontroller icon on the desktop, or select **Start** ⇒**Programs** ⇒**WatchGuard Vcontroller** ⇒ **WatchGuard Vcontroller**.

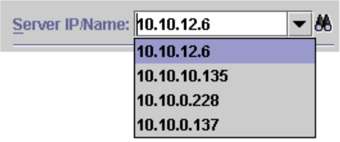
Solaris/Linux

Navigate to the appropriate directory and type `Vcontroller` at the command prompt.

The Vcontroller launches and a login window appears.



If you have used the Vcontroller before to access a Firebox Vclass appliance, the Server IP/Name field displays the IP address or host name of the last accessed appliance.
The IP addresses or host names of other previously accessed devices are listed in the Server IP/Name drop list.



10.10.12.6

10.10.12.6
10.10.10.135
10.10.0.228
10.10.0.137

2 Type the IP address or host name of the Firebox Vclass in the **Server IP/Name** field or select it from the drop list.

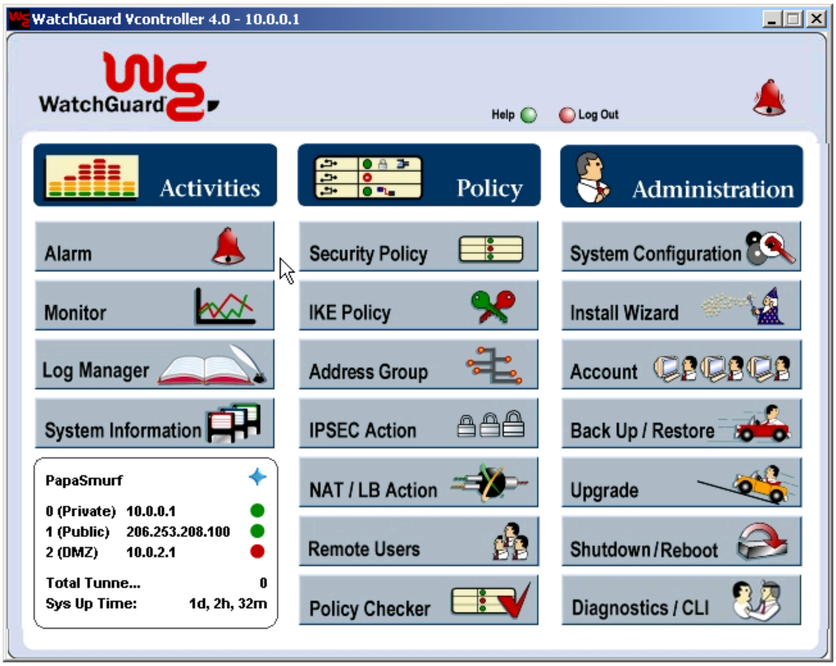
3 Type your administrator login name in the **Name** field.

NOTE

For information on creating administrator accounts, see "Using Account Manager" on page 105.

4 Type the password for your administrator account in the **Password** field.

5 Click **OK**.
The Vcontroller main page appears.



PapaSmurf

0 (Private) 10.0.0.1 ●
1 (Public) 206.253.208.100 ●
2 (DMZ) 10.0.2.1 ●

Total Tunne... 0
Sys Up Time: 1d, 2h, 32m

The Vcontroller Main Page

This section describe the buttons displayed in the Vcontroller.

Activities column buttons

The Activities column contains a series of buttons that, when clicked, provide dialog boxes that update you on system activities. This includes outstanding alarms, recent events, and the current status of the appliance. You can also open a dialog box that displays system logs and another dialog box with a set of useful diagnostic tools.

Alarm

Click this button to open the Alarm Manager window, in which you can define a set of alarms to be triggered when system or policy thresholds are exceeded. This window also allows you to view newly triggered alarms, diagnose alarm conditions, and clear resolved alarms. For more information, see “Using Alarm Manager” on page 231.

Monitor

Click this button to open the **Real-time Monitor** dialog box, which provides a detailed view of the security appliance activities. You can use existing probes, or create your own, to measure system activity as well as to gauge data and policy usage. For more information, see “Monitoring the Firebox Vclass” on page 215.

Log Manager

Click this button to open the **Log Manager** dialog box, which enables you to activate log files that record certain types and levels of system activity. You can also use this dialog box to view a particular log, and then archive your logs as text files for future reference. For more information, see “Using Log Manager” on page 243.

System Information

Click this button to open the **System Information** dialog box, which provides several distinct views of the current appliance’s status and activity. The various tabbed displays are detailed in separate chapters within this guide, depending upon your choice of view. For more information, see “Monitoring the Firebox Vclass” on page 215.

Policy column buttons

The Policy column contains a series of buttons that, when clicked, enable you to create, apply, and manage the security policies used by the Firebox Vclass appliance. For more information on creating policies, see “About Security Policies” on page 113.

Security Policy

Click this button to open the Policy Manager window, which lists the current catalog of security policies. This window allows you to view, edit, add, and remove policies.

IKE Policy
Click this button to open another view of the Policy Manager window that lists the current catalog of IKE policies.

Address Group
Click this button to open a dialog box that shows all the existing address group objects. These are used by both security and IKE policies in determining traffic specifications.

IPSec Action
Click this button to open a dialog box that lists all of the existing IPSec actions, used by security policies to enforce encryption/ authentication protections.

NAT/LB Action (Network Address Translation/Load Balancing Action)
Click this button to open a dialog box that lists all the existing NAT action objects, which are used in policies that affect dynamic IP, virtual IP, and other load-balancing actions on data.

Remote Users
Click this button to open the **RAS Configuration** dialog box, which assists in the setup of remote access service (RAS) connections. This feature is not available on the V10 model.

Policy Checker
Click this button to open a dialog box that enables you to check which policy is applied when a simulated data stream is detected. This dialog box can be used to verify the search order of security policies listed in the Policy Manager window.

Administration column buttons

This column lists a series of buttons that, when clicked, can help customize, monitor, and maintain a Firebox Vclass appliance.

System Configuration
Click this button to open the **System Configuration** dialog box, which helps you change the system configurations of a Firebox Vclass appliance. For more information, see “System Configuration” on page 61.

Install Wizard

Click this button to reopen the Installation Wizard, which you can use to reestablish the basic configuration for a Firebox Vclass appliance if required. For more information, see "Getting Started" on page 17.

Account

Click this button to open the **Account Manager** dialog box, which you can use to modify or add new administrative accounts as well as end-user accounts to allow internal users to bypass any firewall policies you create. For more information, see "Using Account Manager" on page 105.

Backup/Restore

Click this button to open the **Backup/Restore** dialog box, which enables you to back up the current system configuration. You can also use this dialog box to restore previously archived configurations as needed. For more information, see "Backing Up and Restoring Configurations" on page 263.

Upgrade

Click this button to open the **Upgrade** dialog box, which allows you to view the current software version, download and install any recent upgrades, and view the recent upgrade history.

You can also use this dialog box's features to downgrade an appliance to a previous software version. For more information about the **Upgrade** dialog box, see "Upgrading and Downgrading the Software Version" on page 57.

Shutdown/Reboot

Click this button to open a dialog box from which you can restart the software, reboot the appliance, or completely shut down the appliance. For more information, see "Shutting Down and Rebooting" on page 55.

Diagnostics/CLI

Click this button to open the **Diagnostics** dialog box, which includes testing tools, connectivity probes, and a workspace for importing CLI scripts. For more information, see "Monitoring the Firebox Vclass" on page 215.

Page-top buttons

The page-top title area includes the **Log Out** and **Help** buttons, as well as an alarm indicator that is displayed when an alarm has been triggered.

Log Out
Click this button to log out of Vcontroller and disconnect the Management Station from the Firebox Vclass appliance.

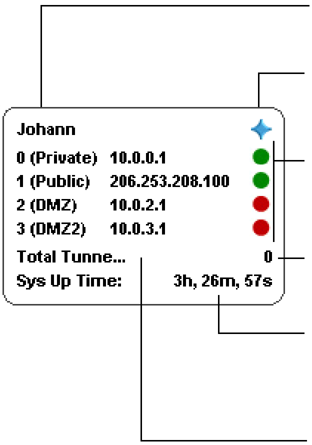
Help
Click this button to open the main online Help window.

Alarm Bell
If you see an animated ringing bell, this indicates that an alarm condition was triggered. Click the alarm bell icon to open the Alarm Manager window. For more information, see "Using Alarm Manager" on page 231.

The status viewer

When you log into the Vcontroller, the status area in the lower-left corner provides a snapshot of the system status, including interface link status and active VPN connections.

From the main Vcontroller page, look for the status indicators in the lower-left corner.



Johann

0 (Private) 10.0.0.1 🟢

1 (Public) 206.253.208.100 🟢

2 (DMZ) 10.0.2.1 🔴

3 (DMZ2) 10.0.3.1 🔴

Total Tunne... 0

Sys Up Time: 3h, 26m, 57s

The system name assigned to this appliance

The refresh button

The current status indicators for the interfaces—green indicates active, red indicates inactive

The total number of currently active tunnels

The total time this appliance has been in continuous operation

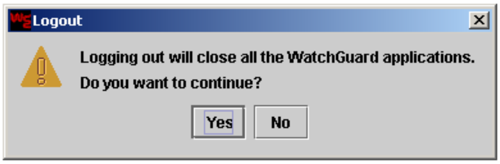
The names and IP addresses of the interfaces

This panel is automatically refreshed every sixty seconds; however, you can click the blue star button to refresh manually.

Logging out of the Vcontroller

Make sure you properly log out of a Firebox Vclass appliance after you finish with administrative tasks. Otherwise, you may have trouble logging in again later because a previous session may still be active.

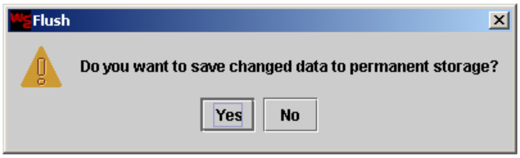
1 From the Vcontroller main page, click **Log Out**.
The Logout confirmation dialog box appears.



Logout

Logging out will close all the WatchGuard applications.
Do you want to continue?

2 Click **Yes**.
If you have made any changes, a Flush dialog box appears requesting to save these to the permanent data storage.

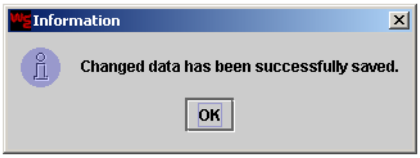


Flush

Do you want to save changed data to permanent storage?

3 To save the changes, click Yes.

An Information dialog box appears indicating that the save was successful.



Information

Changed data has been successfully saved.

4 Click **OK**.

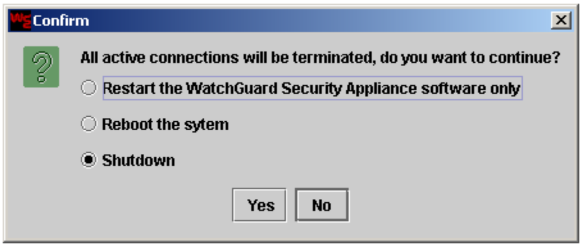
You can now exit Vcontroller or click **Log In** to reconnect to the Firebox Vclass appliance.

Shutting Down and Rebooting

To perform a software shutdown prior to turning off the appliance, follow these instructions:

1 From the main Vcontroller page, click **Shutdown/Reboot**.

A Confirmation dialog box appears.



Confirm

All active connections will be terminated, do you want to continue?

○ Restart the WatchGuard Security Appliance software only

○ Reboot the sytem

● Shutdown

2 Click **Shutdown** and then click **Yes**.

This prompts the Firebox Vclass appliance to quit all software operations and perform a preliminary shutdown of the appliance. While the appliance is shutting down, the Ready LED blinks. After the Ready LED is off, wait 30 seconds.

NOTE

Do not disconnect the power before 30 seconds have elapsed. Disconnecting the appliance too quickly can cause serious damage.

3 After 30 seconds have elapsed, turn off the power switch on the back of the appliance. For the V10 model, simply disconnect the power cord.

4 Unplug the power cord from the Firebox Vclass appliance.

NOTE

Do not remove the cover on the power supply switch on the back of any appliances and use that switch to cut power. This can damage the appliance.

Once you have fully shut down the Firebox Vclass appliance, you can restart it by following these steps:

- Connect the Firebox Vclass appliance to a power source.
- Press the Power switch on the back of the appliance.
  - The Power LED light illuminates, and the Ready LED light starts to blink when the appliance is initializing.
  - When the blinking has stopped and the Ready LED is steadily lit, initialization is complete.
- You can now start the Vcontroller and log into the appliance to perform any administrative work.

To restart the appliance software only, follow these instructions:

- From the main Vcontroller page, click **Shutdown/Reboot**.
- Click **Restart the WatchGuard Security Appliance software only** and then click **Yes**.

  A status dialog box appears and remains on screen until the reboot is complete. After some time elapses, the Vcontroller Login dialog box reappears.

To reboot an appliance without turning off the power, follow these instructions:

- From the main Vcontroller page, click **Shutdown/Reboot**.

- Click **Reboot the system** and then click **Yes**.
  A status dialog box appears and remains on screen until the reboot is complete. After a long interval, the Vcontroller Login dialog box reappears.

Restarting the appliance

You can force a restart by inserting a straight pin into the recessed **Reset** button opening on the front of the appliance.

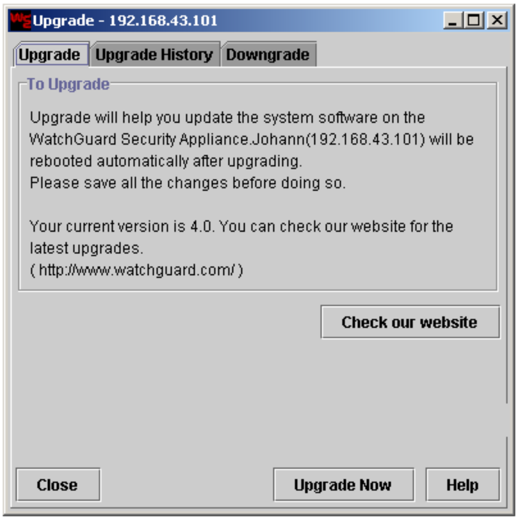
Upgrading and Downgrading the Software Version

When new versions of the Firebox Vclass operating system software become available, the Vcontroller provides a simple way to perform an upgrade procedure.

To upgrade the software version, follow these instructions:

1 Verify that the Management Station has an active Internet connection.
You need an Internet connection to check the WatchGuard Web site for the latest software updates.

2 From the main Vcontroller page, click **Upgrade**.
The Upgrade dialog box appears.



Upgrade will help you update the system software on the WatchGuard Security Appliance.Johann(192.168.43.101) will be rebooted automatically after upgrading.
Please save all the changes before doing so.

Your current version is 4.0. You can check our website for the latest upgrades.
(http://www.watchguard.com/)

3 Note the current version number as reported in the **Upgrade** tab.

4 Click **Check our Web site** to verify whether a more recent version of the Vcontroller software is available.

Your web browser appears and connects to the WatchGuard Web site.

5 When this connection is complete, you can quickly verify the version number of the latest available upgrade against the version number listed in the **Upgrade** tab.

Do not upgrade your appliance until you have backed up the current configuration file. For information on backing up your configuration, see "Backing Up and Restoring Configurations" on page 263.

6 Review the instructions on this Web page. If a newer upgrade is available, click **Download**.

7 When the download is complete, close the browser window and continue with the upgrade procedure.

8 Return to the **Upgrade** dialog box and click **Upgrade Now**.

The Select the upgrading file dialog box appears.

9 Locate and select the downloaded upgrade file and then click **Select**.

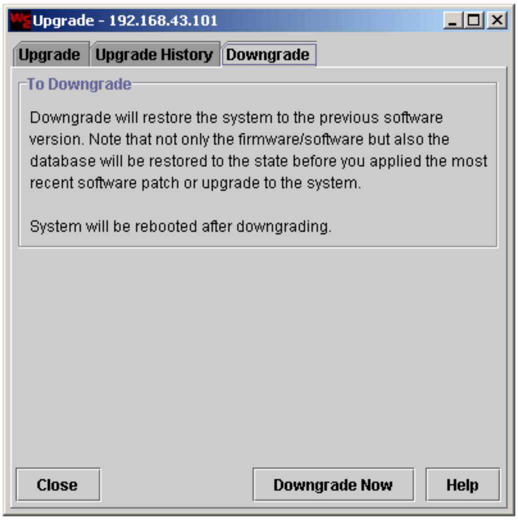
When the upgrade is complete, a confirmation dialog box appears.

10 Click **OK** to proceed.

The Vclass appliance automatically restarts. When the restart is complete, you can log into the appliance and use the Vcontroller to check the upgraded appliance.

To downgrade the software version, follow these instructions:

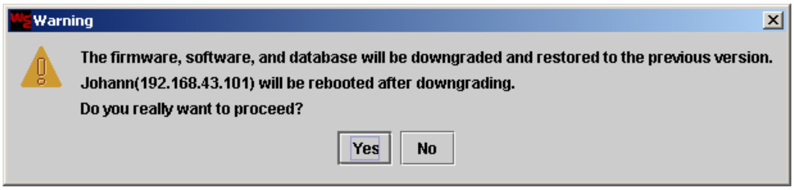
1 Click the **Downgrade** tab.



Downgrade will restore the system to the previous software version. Note that not only the firmware/software but also the database will be restored to the state before you applied the most recent software patch or upgrade to the system.

System will be rebooted after downgrading.

2 Read the instructions on the screen and then click **Downgrade Now**.
A confirmation dialog box appears.



The firmware, software, and database will be downgraded and restored to the previous version.
Johann(192.168.43.101) will be rebooted after downgrading.
Do you really want to proceed?

3 Click **OK**.
The appliance performs the downgrade, and then reboots itself. After the appliance completes the reboot, the Login dialog box automatically appears.

At this time, you may need to restore the last backup of policies and configurations that you saved when this version of the software was in effect. Because a Firebox Vclass appliance stores a maximum of two versions of software, you can only downgrade to the previous version of the software. After this downgrade is complete, your appliance will be using an earlier version of software with the configurations and policies that were in effect at that time. All subsequent entries and changes will be lost.

For information about restoring older settings, see “Restoring an Archived Configuration” on page 265.

The Upgrade History

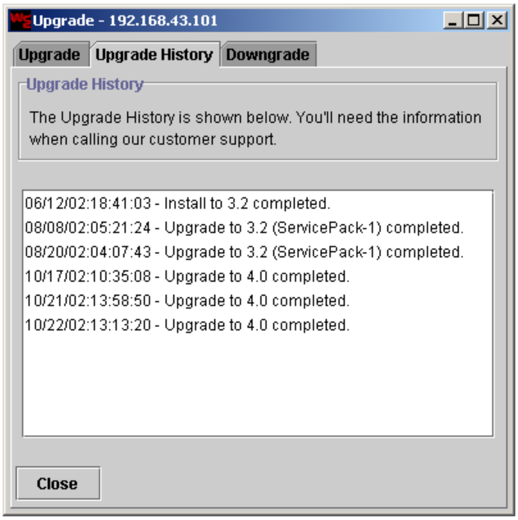
The **Upgrade History** tab notes the dates, times, and version numbers of all occasions when the Firebox Vclass appliance has been upgraded or downgraded. The upgrade history remains even if the Vclass appliance is restored to the factory default.

To view the upgrade history:

1 Launch Vcontroller and log into the appliance.

2 Click **Upgrade**.
The Upgrade dialog box appears.

3 Click the **Upgrade History** tab.



The Upgrade History is shown below. You'll need the information when calling our customer support.

```
06/12/02:18:41:03 - Install to 3.2 completed.
08/08/02:05:21:24 - Upgrade to 3.2 (ServicePack-1) completed.
08/20/02:04:07:43 - Upgrade to 3.2 (ServicePack-1) completed.
10/17/02:10:35:08 - Upgrade to 4.0 completed.
10/21/02:13:58:50 - Upgrade to 4.0 completed.
10/22/02:13:13:20 - Upgrade to 4.0 completed.
```

Transferring from the Vcontroller to WatchGuard CPM

If you need to transfer the management of the Firebox Vclass from the Vcontroller to the WatchGuard CPM, consider the following differences between the two environments:

- Vcontroller provides management access to more built-in functionality in Firebox Vclass appliances than CPM. For example, you cannot use the Firebox Vclass appliance for RAS user authentication in CPM as you can with Vcontroller; only a RADIUS server can be used. However, if you have five or more Firebox Vclass appliances, CPM is the preferred global management tool.
- You cannot use both Vcontroller and CPM to manage the same appliances. If you use CPM to deploy a complete profile, any changes that are made later with Vcontroller will be erased when a new or updated profile is deployed to that appliance from CPM.

CHAPTER 5

System Configuration

Use the **System Configuration** dialog box to enter or edit system settings. This dialog box, a key component of the Vcontroller, provides one-stop access to a wide spectrum of controls, ranging from network connection parameters to an array of hacker prevention options.

General Configuration

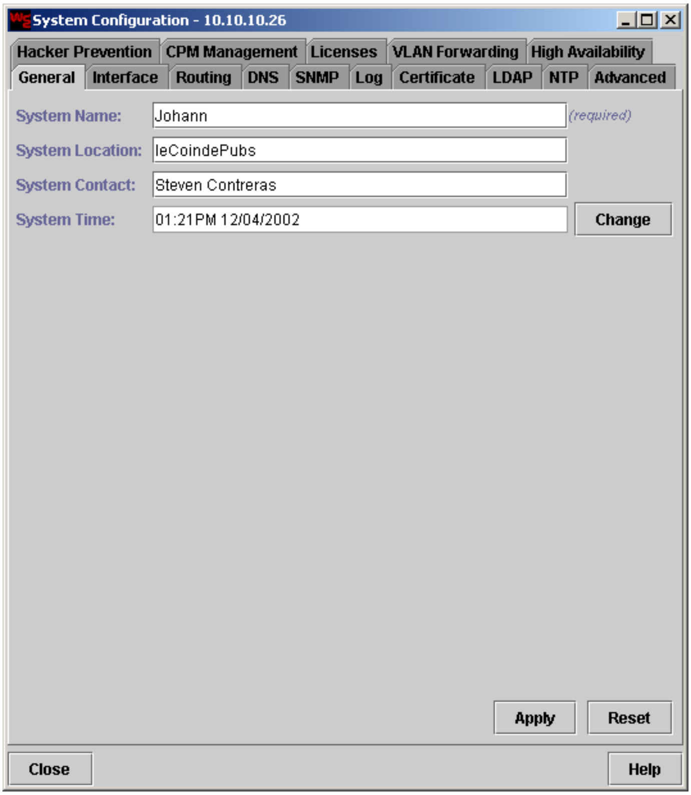
Use the **General** tab to fill in general information about the Vclass name, location, and owner, and to set the system time.

1 From the main Vcontroller page, click **System Configuration**.

The System Configuration dialog box appears.

2 Click the **General** tab.

The General system settings are displayed.



System Name: Johann (required)

System Location: leCoindePubs

System Contact: Steven Contreras

System Time: 01:21PM 12/04/2002

Configure the following system settings:

System Name

Type a name to represent this appliance.

System Location

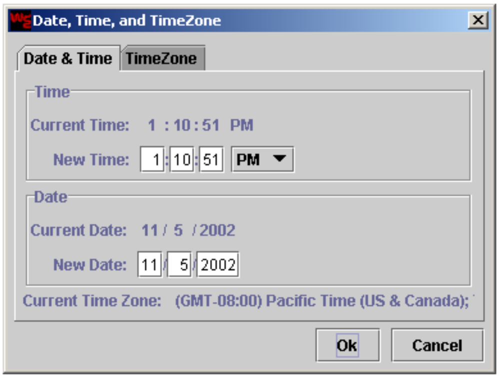
Type the location of your Firebox Vclass appliance. The location can be a building and floor number, or a simple identifier such as “LAN Room.”

System Contact

Type the name, phone number, or email address of the principal system administrator or the person responsible for maintenance of the Firebox Vclass system.

System Time

Displays the current date and time. To change the date and time currently displayed, click **Change**. The **Date, Time, and Time Zone** dialog box appears.



Current Time: 1 : 10 : 51 PM

New Time: 1 : 10 : 51 PM

Current Date: 11 / 5 / 2002

New Date: 11 / 5 / 2002

Current Time Zone: (GMT-08:00) Pacific Time (US & Canada);

- Click the **Date & Time** tab and then type the appropriate time and date for your system. Select **AM** or **PM** from the drop list.
- Click the **TimeZone** tab to update the geographic location of your system. Select the appropriate location from the list and then click **OK** to return to the **General** tab.

When you have finished configuring the system settings, click one of the following options:

Reset

To return the settings to the previous configuration.

Apply

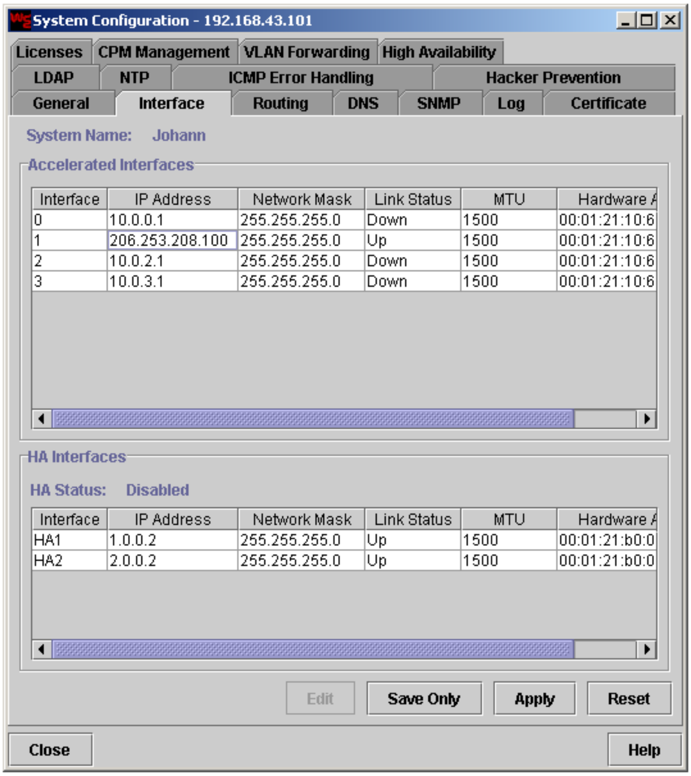
To immediately commit the settings to the Firebox Vclass appliance.

Interface Configuration

The **Interface** tab is used to make changes to the IP addresses and subnet masks of the interfaces. Different combinations of interfaces are displayed according to the model of Firebox Vclass appliance you are configuring.

- Click the **Interface** tab.

  The Interface settings are displayed. In this example, the interfaces for the V60 and V80 models are shown.



System Name: Johann

Accelerated Interfaces

Interface	IP Address	Network Mask	Link Status	MTU	Hardware A
0	10.0.0.1	255.255.255.0	Down	1500	00:01:21:10:6
1	206.253.208.100	255.255.255.0	Up	1500	00:01:21:10:6
2	10.0.2.1	255.255.255.0	Down	1500	00:01:21:10:6
3	10.0.3.1	255.255.255.0	Down	1500	00:01:21:10:6

HA Interfaces

HA Status: Disabled

Interface	IP Address	Network Mask	Link Status	MTU	Hardware A
HA1	1.0.0.2	255.255.255.0	Up	1500	00:01:21:b0:0
HA2	2.0.0.2	255.255.255.0	Up	1500	00:01:21:b0:0

- Both the Accelerated Interfaces and the HA (High Availability) Interfaces are listed:

  Interface 0

  This represents interface 0, which should be used for all private, or trusted, network traffic.

  Interface 1

  This represents interface 1, which should be used for all public, or external, network traffic.

  Interface 2

  Interface 2 should be assigned to any DMZ network traffic. This interface is not available on the V10 or V100 models.

Interface 3

Interface 3 should be assigned to any DMZ network traffic. This interface is not available on the V10 or V100 models.

Interfaces HA1 and HA2

Certain Firebox Vclass appliance models include two HA ports, HA1 and HA2. HA ports are used with the High Availability feature, which allows for redundancy and transparent failover in the case of a hardware failure. HA ports are connected between Vclass appliances, and not to the network. The HA2 ports can be connected to each other for greater redundancy, or you can use the HA2 ports as direct management connections. For more information, see “Setting Up a High Availability System” on page 283.

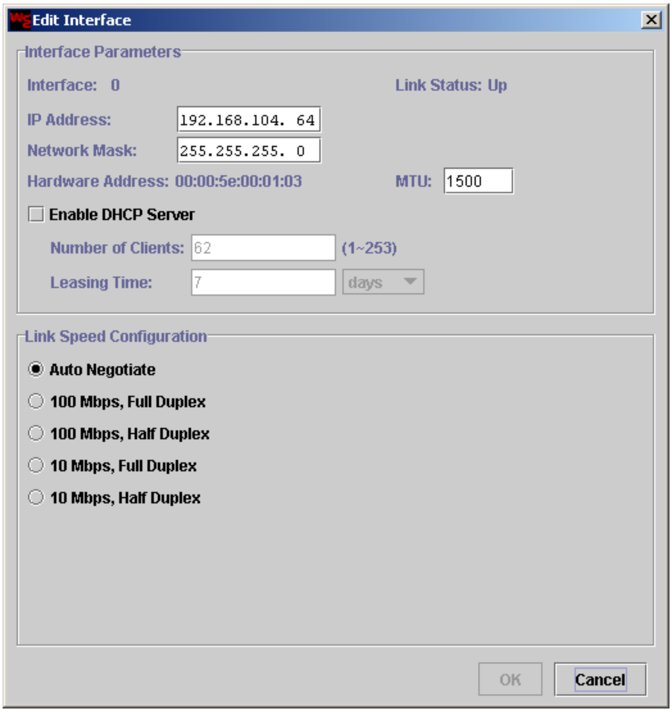
This interface is not available on the V10 model.

If you need to make any changes to the configuration of the interfaces, use the following instructions.

Configuring Interface 0

To edit the interface settings, follow these steps:

1 Select the interface entry and then double-click.
The Edit Interface dialog box appears.



Edit Interface

Interface Parameters

Interface: 0

Link Status: Up

IP Address: 192.168.104. 64

Network Mask: 255.255.255. 0

Hardware Address: 00:00:5e:00:01:03

MTU: 1500

□ Enable DHCP Server

Number of Clients: 62 (1~253)

Leasing Time: 7 days

Link Speed Configuration

● Auto Negotiate

○ 100 Mbps, Full Duplex

○ 100 Mbps, Half Duplex

○ 10 Mbps, Full Duplex

○ 10 Mbps, Half Duplex

2 Type the IP address and network mask in the appropriate fields.
The interface Hardware Address (MAC address) is displayed beneath these fields.

3 Type a MTU to determine the maximum size of each packet. The default is 1500.

4 If you want to enable the appliance as a DHCP server, click the checkbox labeled **Enable DHCP Server**.
This option is not available if you are using High Availability.

5 Type the maximum number of potential clients that will be assigned IP addresses in the **Number of Clients** field.

6 Select either **Days** or **Hours** from the **Leasing Time** drop list.

7 Type the number of hours or days that an IP address will be loaned to a DHCP client.

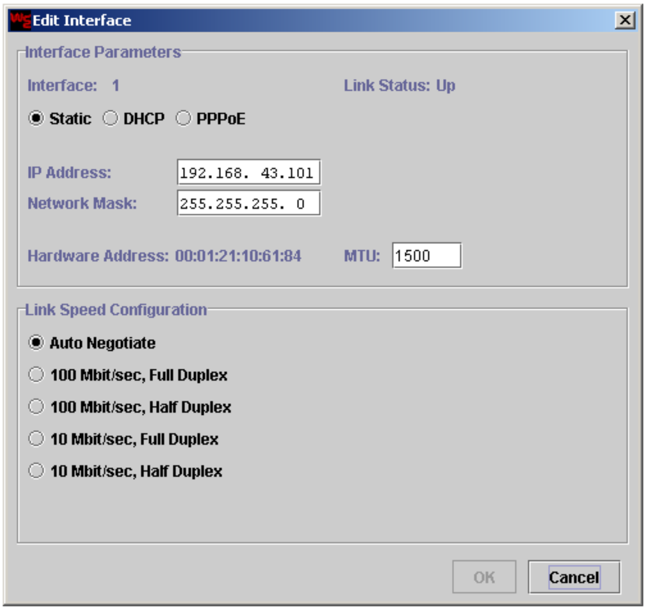
8 Click the Link Speed Configuration option you want to use for this interface. The default is Auto Negotiate. This default value is the only option available on the V100 model.

9 Click **OK** to close the **Edit Interface** dialog box and return to the **Interface** tab.

Configuring Interface 1

To edit the interface settings, follow these steps:

1 Select the interface entry and then double-click.
The Edit Interface dialog box appears.



Edit Interface

Interface Parameters

Interface: 1
Link Status: Up

● Static ○ DHCP ○ PPPoE

IP Address: 192.168. 43.101
Network Mask: 255.255.255. 0

Hardware Address: 00:01:21:10:61:84
MTU: 1500

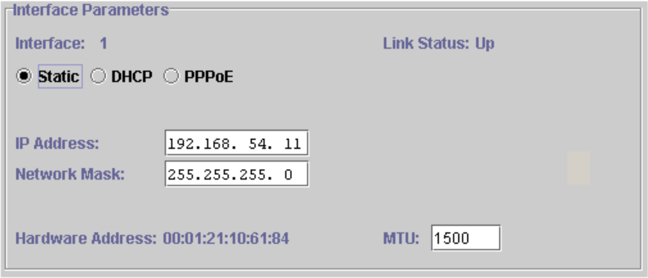
Link Speed Configuration

● Auto Negotiate
○ 100 Mbit/sec, Full Duplex
○ 100 Mbit/sec, Half Duplex
○ 10 Mbit/sec, Full Duplex
○ 10 Mbit/sec, Half Duplex

Interface 1 (Public) allows you to choose from the following three network addressing options:

Static

Type the IP address and network mask in the appropriate fields.



Interface Parameters

Interface: 1

Link Status: Up

● Static ○ DHCP ○ PPPoE

IP Address: 192.168. 54. 11

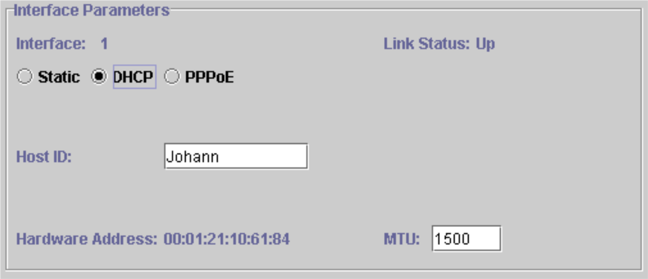
Network Mask: 255.255.255. 0

Hardware Address: 00:01:21:10:61:84

MTU: 1500

DHCP

Type the host name or the IP address of your DHCP server in the **Host ID** field.



Interface Parameters

Interface: 1

Link Status: Up

○ Static ● DHCP ○ PPPoE

Host ID: Johann

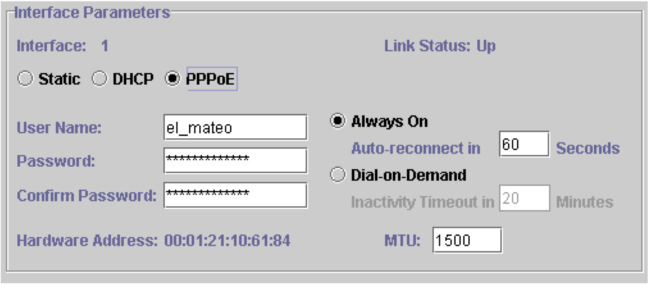
Hardware Address: 00:01:21:10:61:84

MTU: 1500

This option is not available when using High Availability.

PPPoE

Type the user name and password in the appropriate fields. Type the password again to confirm it. Select the **Always On** or **Dial-on-Demand** option and then type the desired time interval in the appropriate field.



Interface Parameters

Interface: 1

Link Status: Up

○ Static ○ DHCP ● PPPoE

User Name: el_mateo

Password: **************

Confirm Password: **************

● Always On

Auto-reconnect in 60 Seconds

○ Dial-on-Demand

Inactivity Timeout in 20 Minutes

Hardware Address: 00:01:21:10:61:84

MTU: 1500

This option is not available when using High Availability.

2 Type a MTU to determine the maximum size of each packet. The default is 1500.

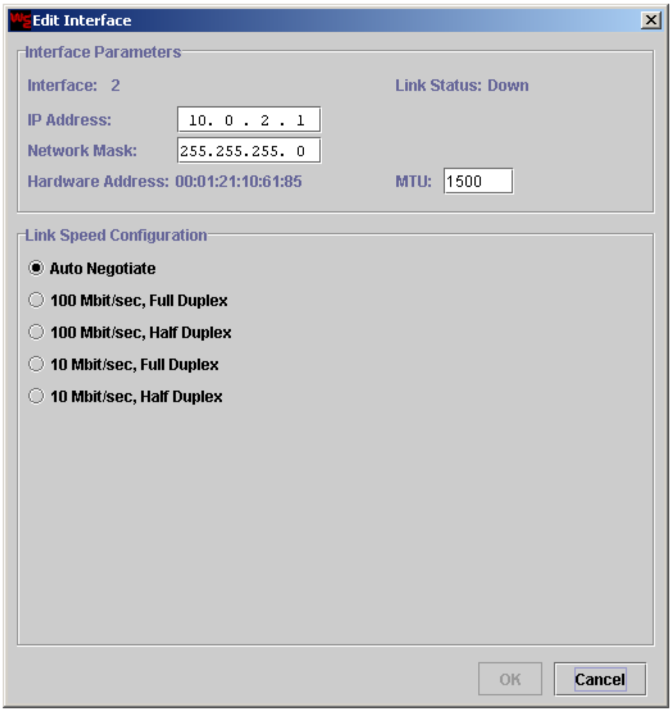
3 Click the Link Speed Configuration option you want to use for this interface. The default is Auto Negotiate. This default value is the only option available on the V100 model.

4 Click **OK** to close the **Edit Interface** dialog box and return to the Interface tab.

Configuring Interface 2 or 3

To edit the interface settings, follow these steps:

1 Select the interface entry and then double-click.
The Edit Interface dialog box appears.



Edit Interface

Interface Parameters

Interface: 2

Link Status: Down

IP Address: 10. 0 . 2 . 1

Network Mask: 255.255.255. 0

Hardware Address: 00:01:21:10:61:85

MTU: 1500

Link Speed Configuration

● Auto Negotiate

○ 100 Mbit/sec, Full Duplex

○ 100 Mbit/sec, Half Duplex

○ 10 Mbit/sec, Full Duplex

○ 10 Mbit/sec, Half Duplex

2 Type the IP address and network mask in the appropriate fields.
The interface Hardware Address (MAC address) is displayed beneath these fields.

3 Type a MTU to determine the maximum size of each packet. The default is 1500.

4 Click the Link Speed Configuration option you want to use for this interface. The default is Auto Negotiate. This default value is the only option available on the V100 model.

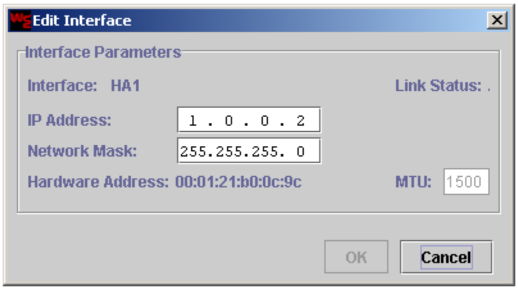
5 Click **OK** to close the **Edit Interface** dialog box and return to the **Interface** tab.

Configuring the HA Interfaces

For more information on setting up and managing these HA interfaces, see “Setting Up a High Availability System” on page 283.

To edit High Availability settings, follow these steps:

1 Select the interface entry and then double-click.
The Edit Interface dialog box appears.



Interface: HA1

Link Status: .

IP Address: 1 . 0 . 0 . 2

Network Mask: 255.255.255. 0

Hardware Address: 00:01:21:b0:0c:9c

MTU: 1500

2 Type the IP address and network mask in the appropriate fields.
The interface Hardware Address (MAC address) is displayed beneath these fields.

3 Type a MTU to determine the maximum size of each packet. The default is 1500.

4 Click **OK** to close the **Edit Interface** dialog box and return to the Interface tab.

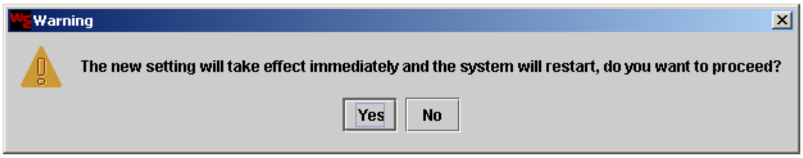
When you have finished configuring the interfaces, click one of the following options:

Reset
To return the settings to the previous configuration

Save Only
To save the settings to the Management Station and apply them to the Firebox Vclass appliance when it is restarted. When you are finished, click **Close**.

Apply
To immediately commit the settings to the Firebox Vclass appliance.

A Warning dialog box appears alerting you that this action forces a restart of the system.


Warning

The new setting will take effect immediately and the system will restart, do you want to proceed?

- Click **Yes** to proceed.

The appliance immediately restarts in order to apply the new interface configurations. The System Configuration dialog box closes and the Vcontroller displays the Log In dialog box.

NOTE

If you have changed the Interface 0 (Private) settings, be sure to use the new IP address when next logging in to Vcontroller.

Routing Configuration

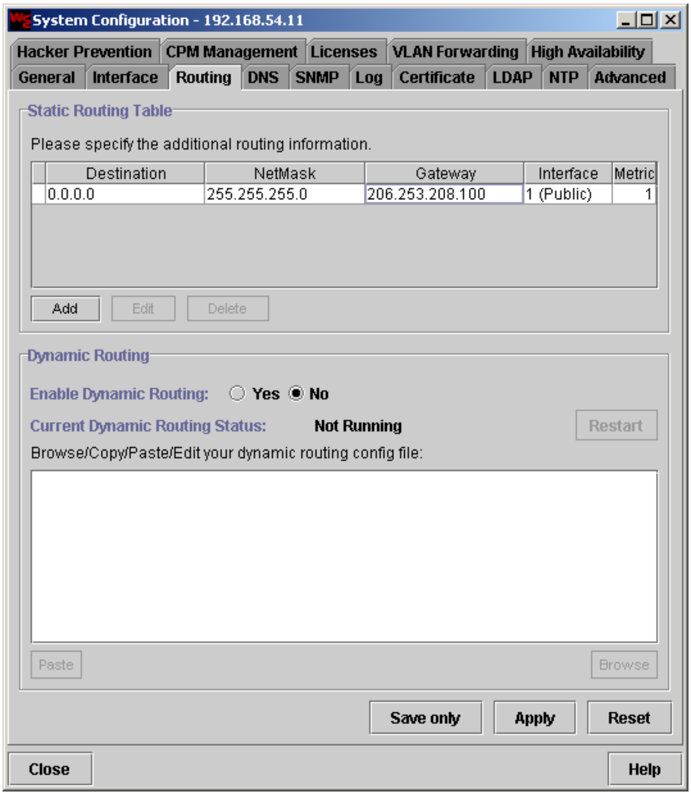
Use the **Routing** tab to record static routes or set up dynamic routing using RIP, RIP version 2, and OSPF.

Configuring static routing

To add static routes, follow these steps:

1 Click the **Routing** tab.

Both the static and dynamic routing settings are displayed.



Static Routing Table

Please specify the additional routing information.

Destination	NetMask	Gateway	Interface	Metric
0.0.0.0	255.255.255.0	206.253.208.100	1 (Public)	1

Dynamic Routing

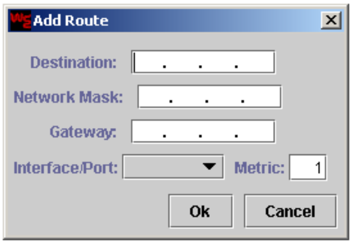
Enable Dynamic Routing: ○ Yes ● No

Current Dynamic Routing Status: Not Running

Browse/Copy/Paste/Edit your dynamic routing config file:

2 To configure a static route, click **Add**.

The Add Route dialog box appears.



Destination: . . .

Network Mask: . . .

Gateway: . . .

Interface/Port:

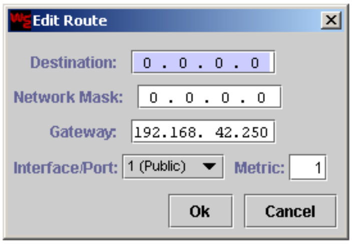
Metric: 1

3 Type the destination, network mask, gateway, and metric in the appropriate fields. Select the interface from the drop list and then click **OK**.

Repeat this process to add other static route entries.

4 To modify an existing route, select the entry and click **Edit**.

The Edit Route dialog box appears



Edit Route

Destination: 0 . 0 . 0 . 0

Network Mask: 0 . 0 . 0 . 0

Gateway: 192.168. 42.250

Interface/Port: 1 (Public) Metric: 1

5 Click **OK**.

Configuring dynamic routing

To configure dynamic routing follow these steps:

1 To enable dynamic routing, click **Yes**.

If you later decide to disable dynamic routing, click **No**.

2 Click **Paste** to insert a preconfigured dynamic routing configuration file into the text field or click **Browse** to locate the file on your management station.

It is possible that dynamic routing can go down. If this occurs, the Current Gated Status displays “Not Running.”

1 Click **Restart**.

A Confirmation dialog box appears.

2 Click **Yes** to restart.

When you have finished configuring routing, click one of the following options:

Reset

To return the settings to the previous configuration.

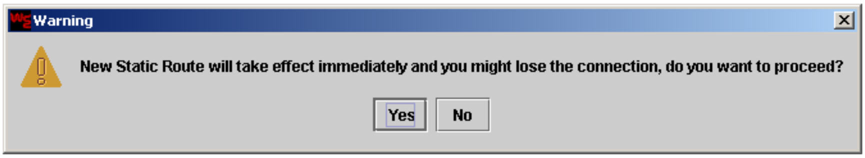
Save Only

To save the settings to the Management Station and apply them to the Firebox Vclass appliance when it is restarted. When you are finished, click **Close**.

Apply

To immediately commit the settings to the Firebox Vclass appliance.

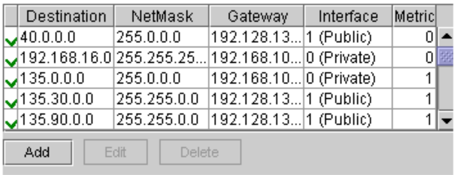
A Warning dialog box appears.



New Static Route will take effect immediately and you might lose the connection, do you want to proceed?

- Click **Yes** to proceed.

At this time, the Firebox Vclass checks your entries for accuracy. If the entry is correct, a green checkmark appears to the left of the new routing table entry. If the entry is incorrect, a red X appears.



	Destination	NetMask	Gateway	Interface	Metric
✓	40.0.0.0	255.0.0.0	192.128.13...	1 (Public)	0
✓	192.168.16.0	255.255.25...	192.168.10...	0 (Private)	0
✓	135.0.0.0	255.0.0.0	192.168.10...	0 (Private)	1
✓	135.30.0.0	255.255.0.0	192.128.13...	1 (Public)	1
✓	135.90.0.0	255.255.0.0	192.128.13...	1 (Public)	1

If an entry displays a red X, click the **Routing Table Edit** button to open the **Edit Route** dialog box. The box allows you to check the text for errors.

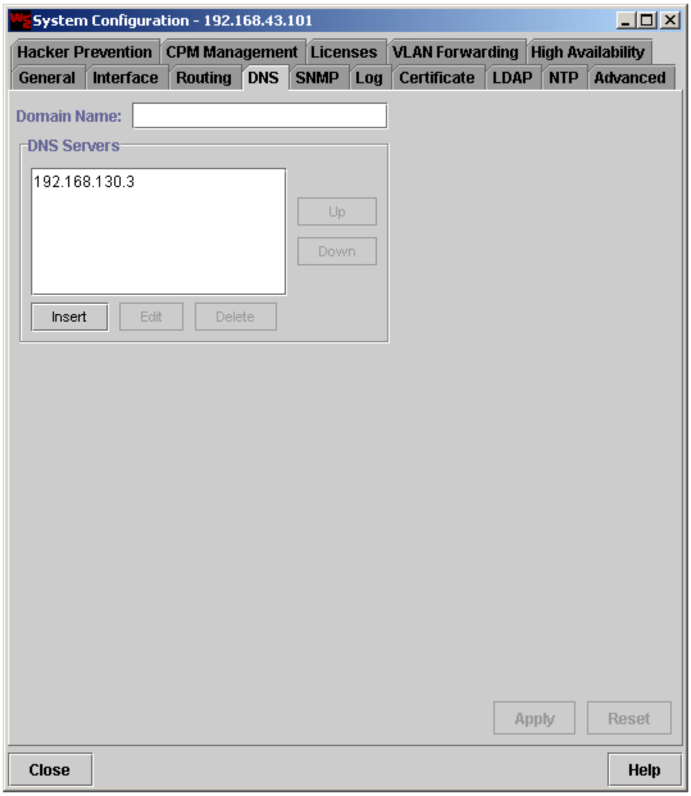
DNS Configuration

Use the **DNS** tab to configure the Firebox Vclass appliance with a host domain name and DNS server entries.

To configure a system domain name, follow these steps:

1 Click the **DNS** tab.

The DNS settings are displayed.



Domain Name:

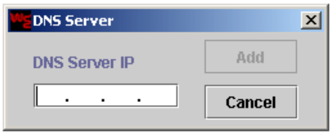
DNS Servers

192.168.130.3

2 Type the domain name of the Firebox Vclass appliance in the appropriate field.

To add a DNS server, follow these steps:

1 Click **Insert**.
The DNS Server dialog box appears.



2 Type the IP address in the appropriate field.

3 Click **Add**.

The DNS Server dialog box closes and the new server IP address appears in the DNS Server list.

To manage the DNS server entries, follow these instructions:

- To edit a DNS server IP address, select the entry from the DNS Server List and click **Edit**.
- To delete a DNS server IP address, select the entry from the DNS Server List and click **Delete**.
- If you have more than one server in the list, you can reorganize the search order by choosing a server entry and then clicking **Up** or **Down**.

When you have finished configuring the DNS settings, click one of the following options:

Reset

To return the settings to the previous configuration.

Apply

To immediately commit the settings to the Firebox Vclass appliance.

SNMP Configuration

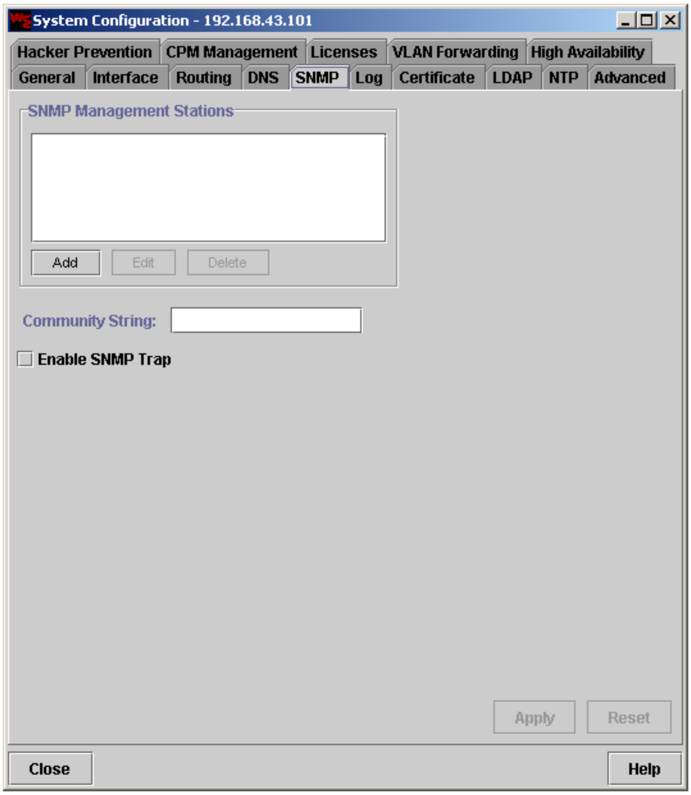
Use the **SNMP** tab to add the IP addresses of management stations that will be monitoring this appliance. You also use these fields to record the relevant SNMP community string. For a complete list of supported MIBs for Firebox Vclass appliances, review the MIB files that are stored on the WatchGuard CD.

Because Firebox Vclass appliances support the SNMP version 1 protocol, you can assign an SNMP community to this Firebox Vclass appliance so that it can be managed through SNMP management stations. You can also configure this appliance so that an SNMP trap will be sent to all related management stations when an alarm is triggered. However, to retrieve SNMP MIB counters from a Firebox Vclass appliance, you must first create and apply a security policy that allows SNMP traffic to pass through the appliance.

To configure SNMP traps, follow these steps:

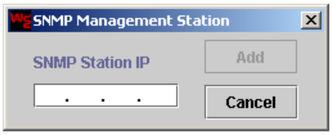
1 Click the **SNMP** tab.

The SNMP settings are displayed.



2 Click **Add**.

The SNMP Management Station dialog box appears.



3 Type the IP address in the appropriate field.

4 Click **Add**.

Repeat this process to record the IP addresses of all other management stations.

5 Type the password that will identify the appliance to the Management Station or stations in the **Community String** field.
This step is optional.

6 Click **Enable SNMP Trap**.

NOTE

Although no traps are sent if the Enable SNMP Trap option is disabled, triggered alarms are still logged by the appliance.

When you have finished configuring the SNMP management stations, click one of the following options:

Reset
To return the settings to the previous configuration.

Apply
To immediately commit the settings to the Firebox Vclass appliance.

Log Configuration

Use the **Log** tab to configure the logging settings. For information on configuring these settings, see “Log Settings” on page 247.

Certificate Configuration

If you plan to use this Firebox Vclass appliance to manage VPN connections that incorporate automatic (IKE) key exchanges, you must purchase an x.509 authorization certificate from a Certificate Authority (CA) server (such as *Verisign* or *Entrust*), and then import it into your Firebox Vclass appliance. Use the **Certificate** tab to configure these certificates.

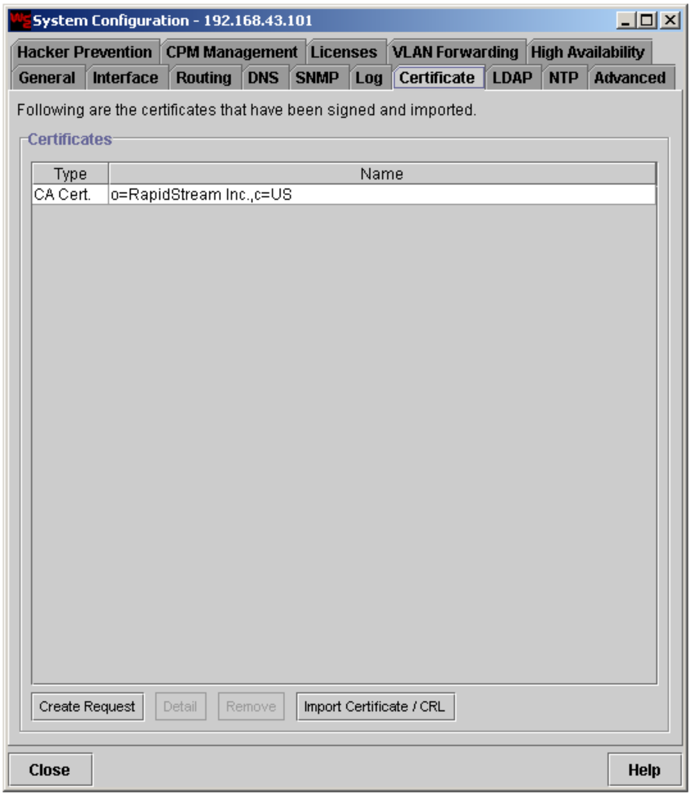
In addition, this tab assists in the importing of Certificate Revocation Lists (CRLs), which the authorizing source will send to you on occasion. A CRL effectively cancels any certificates that have been compromised by hackers.

Before initiating a certificate request, you must obtain the following:

- The encryption key cosigning authority's name and web site URL
- A payment method for all requested certificates, preferably credit card
- Any root certificates provided by this authority

To import certificates, follow these steps:

1 Click the **Certificate** tab.
The Certificate fields are displayed. A default WatchGuard certificate is imported by default.

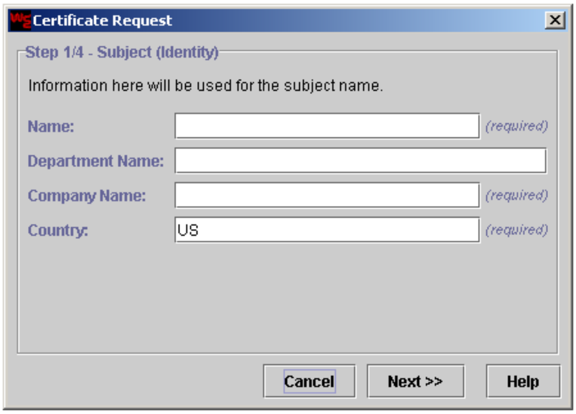


Following are the certificates that have been signed and imported.

Certificates

Type	Name
CA Cert.	o=RapidStream Inc.,c=US

2 To request a new x.509 certificate, click **Create Request**.
The Certificate Request dialog box appears.



Certificate Request

Step 1/4 - Subject (Identity)

Information here will be used for the subject name.

Name: (required)

Department Name:

Company Name: (required)

Country: US (required)

3 Type the following information:

Name
The name of the Firebox Vclass appliance. This is the same as the system name configured in the General settings. See “General Configuration” on page 61.

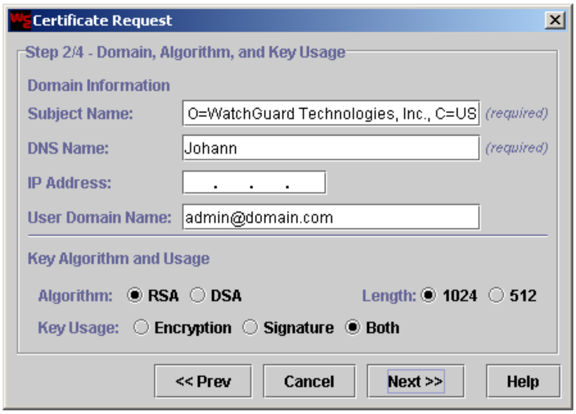
Department Name
The group or department name that administers this appliance. This field is optional.

Company Name
The company name.

Country
The name of the country in which this appliance and the certificate will be used.

4 Click **Next.**

The next certificate request dialog box appears, as shown in the following figure.



Step 2/4 - Domain, Algorithm, and Key Usage

Domain Information

Subject Name: O=WatchGuard Technologies, Inc., C=US (required)

DNS Name: Johann (required)

IP Address: . . .

User Domain Name: admin@domain.com

Key Algorithm and Usage

Algorithm: ● RSA ○ DSA Length: ● 1024 ○ 512

Key Usage: ○ Encryption ○ Signature ● Both

5 Fill in the following information and click **Next**.

Subject Name
This field is automatically updated with processed data from your first step entries. You can make any deletions or changes in this text field if you know the proper formatting for all the elements.

DNS Name
Type the appliance name or domain name—for example, “wg001.corporation.com”.

IP Address
Type the IP address of interface 0 (Public). This step is optional.

User Domain Name
Type the user name of this appliance. This step is optional.

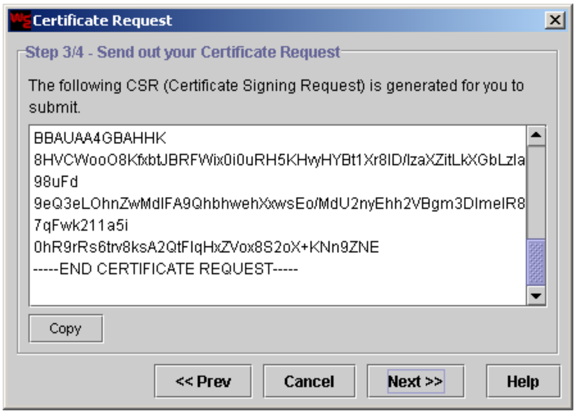
Algorithm
Click the preferred option for this certificate.

Length
Click the preferred option.

Key Usage
Click the preferred option. (If you chose DSA as the algorithm, you can only select Signature for key usage.)

6 Click **Next**.

The Certificate Signing Request (CSR) is displayed.



Step 3/4 - Send out your Certificate Request

The following CSR (Certificate Signing Request) is generated for you to submit.

```
BBAUAA4GBAHHK
8HVCWooO8KfxbtJBRFWix0i0uRH5KHwyHYBt1Xr8ID/lzaXZitLkXGbLzla
98uFd
9eQ3eLOhnZwMdIFA9QhbhwehXxwsEo/MdU2nyEhh2VBgm3DImeIR8
7qFwk211a5i
0hR9rRs6trv8ksA2QtFIqHxZVox8S2oX+KNn9ZNE
-----END CERTIFICATE REQUEST-----
```

7 Select the text in the dialog box and then press `Control+a`.

8 Click **Copy**.

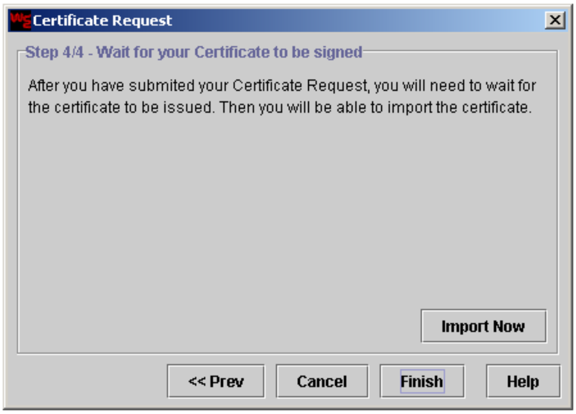
9 Open a Web browser and connect to the Web site of your key co-signing authority.

10 Open the key co-signing authority certificate request form and paste the text into the appropriate field.

11 Provide any other required payment information.

12 Submit the request and then close the browser window.

13 Return to the Certificate Request dialog box and click **Next**.
The final step is displayed.



Step 4/4 - Wait for your Certificate to be signed

After you have submited your Certificate Request, you will need to wait for the certificate to be issued. Then you will be able to import the certificate.

14 Review the information displayed in the **Certificate Request** dialog box, and then click **Finish**.

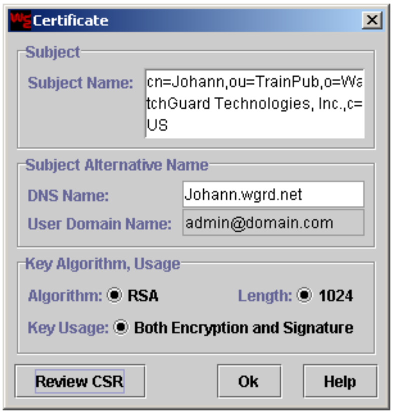
The Certificate Request dialog box closes and the System Configuration dialog box returns. A new entry appears in the Certificate list representing the pending certificate request.

To view specific information about a pending certificate, follow these steps:

1 Select the entry from the **Certificates** list.

2 Click **Detail**.

A Certificate dialog box appears that summarizes all the relevant certificate information.



Certificate

Subject

Subject Name: cn=Johann,ou=TrainPub,o=WatchGuard Technologies, Inc.,c=US

Subject Alternative Name

DNS Name: Johann.wgrd.net

User Domain Name: admin@domain.com

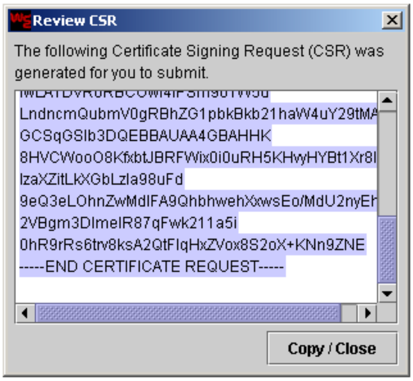
Key Algorithm, Usage

Algorithm: ● RSA Length: ● 1024

Key Usage: ● Both Encryption and Signature

3 Click **Review CSR** to view the Certificate Signing Request.

The Review CSR dialog box appears.



Review CSR

The following Certificate Signing Request (CSR) was generated for you to submit.

```
IWLATDVR0RBCOWI4IFSm90TW5d
LndncmQubmV0gRBhZG1pbkBkb21haW4uY29tMA
GCSqGSIb3DQEBBAUAA4GBAHHK
8HVCWooO8KfxbtJBRFWix0i0uRH5KHvyHYBt1Xr8l
IzaXZitLkXGbLzla98uFd
9eQ3eLOhnZwMdIFA9QhbhwehXxwsEo/MdU2nyEh
2VBgm3DImeIR87qFwk211a5i
0hR9rRs6trv8ksA2QtFIqHxZVox8S2oX+KNn9ZNE
-----END CERTIFICATE REQUEST-----
```

4 Click **Copy/Close** to return to the **Review CSR** dialog box.
A copy of the CSR is sent to the clipboard.

5 Click **OK** when you are finished.

You must wait for the certificate to arrive in the form of a text file from the co-signing authority. When you have received it, follow the instructions in the next procedure.

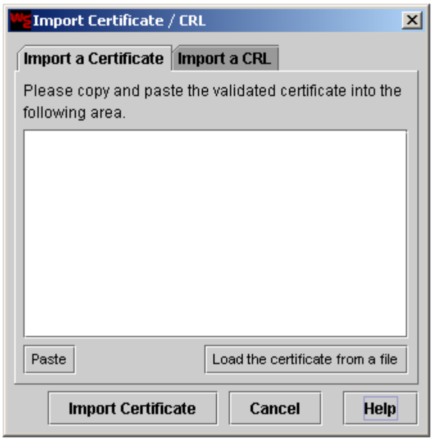
Importing a certificate or CRL file

If this is your first certificate import, you must import the root certificate before importing the actual certificate, or the new x.509 certificate (and any others you subsequently import) will not be usable.

To import the root certificate, follow these steps:

1 Make sure that the root certificate file is present in a local directory.

2 Click **Import Certificate/CRL**.
The Import Certificate/CRL dialog box appears.



Please copy and paste the validated certificate into the following area.

3 Click **Load the certificate from a file**.

4 Locate and select the root certificate file.

NOTE

If you prefer, you can also use a text editor to open the file. Then copy and paste the text.

5 When the certificate text is displayed, click **Import Certificate**.

This imports the certificate into the Firebox Vclass appliance. After the import is complete, the dialog box closes and the newly imported certificate appears in the Certificates list.

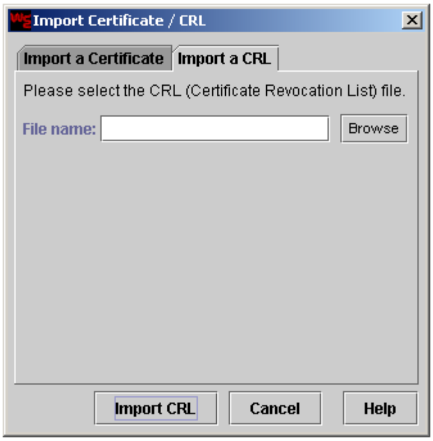
6 Repeat this process to import any other certificates into the Firebox Vclass appliance.

At regular intervals, your key cosigning authority will issue a Certificate Revocation List (CRL), which nullifies any existing certificates that have been compromised. You can import these lists so that your system will not attempt to use any revoked certificates for key exchanges.

To import a CRL, follow these steps:

1 Open the **Import Certificate/CRL** dialog box.

2 Click the **Import a CRL** tab.



Please select the CRL (Certificate Revocation List) file.

File name:

3 Click **Browse**.

4 Locate and select the appropriate CRL file.

5 When the file path appears in the **File Name** field, click **Import CRL**.

This imports the CRL into the Firebox Vclass appliance. After the import is complete, the dialog box closes and the newly imported CRL name appears in the Certificates list.

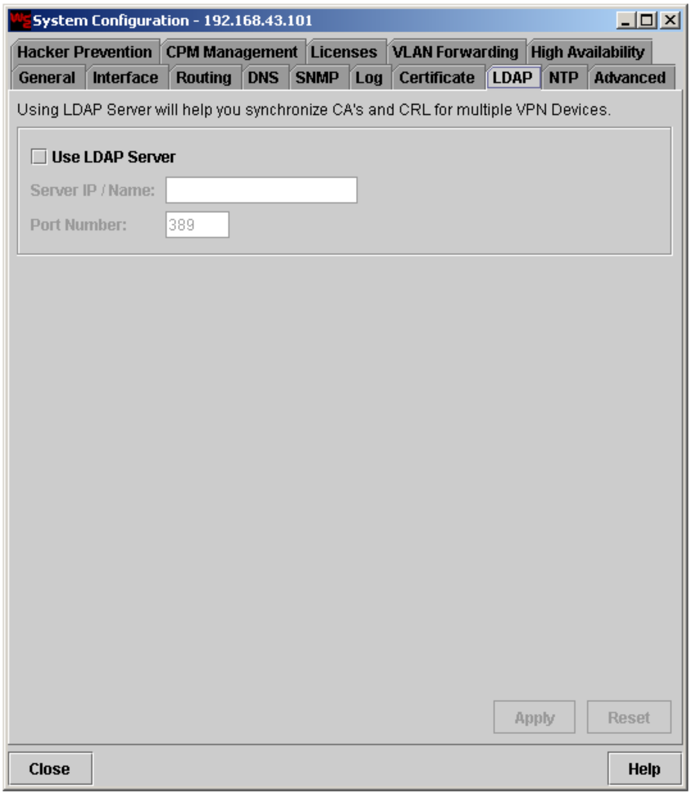
6 To remove an entry from the **Certificate** list, select the entry and click **Remove**.

LDAP Server Configuration

Use the **LDAP** tab to set up a connection between a Firebox Vclass appliance and any LDAP server on which Certificate Revocation List (CRL) files are centrally stored. After this configuration has been set up, the Firebox Vclass appliance can verify every certificate it uses against the CRLs stored in the server. This provides additional protection against compromised certificates.

1 Click the **LDAP** tab.

The LDAP settings are displayed.



Using LDAP Server will help you synchronize CA's and CRL for multiple VPN Devices.

□ Use LDAP Server

Server IP / Name:

Port Number: 389

2 Click the checkbox labeled **Use LDAP Server**.

3 Type the IP address or domain name of the LDAP server in the appropriate field.

4 If the LDAP server is not using the default port number 389, type the correct port number in the appropriate field.

When you have finished configuring the LDAP server settings, click one of the following options:

Reset
To return the settings to the previous configuration.

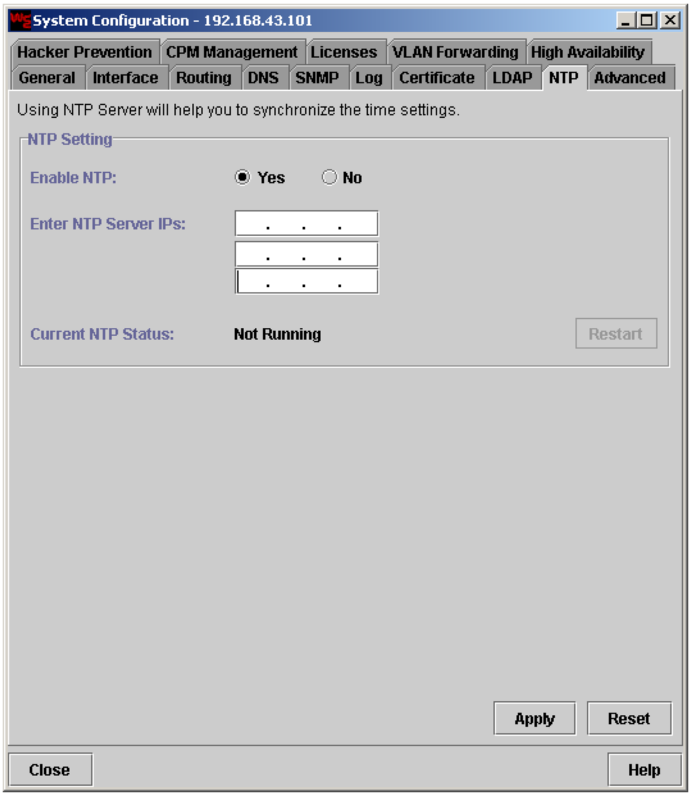
Apply
To immediately commit the settings to the Firebox Vclass appliance.

NTP Server Configuration

Use the **NTP** tab to configure the Firebox Vclass to contact a NTP server. A NTP server uses Coordinated Universal Time (UTC) to synchronize computer clock times.

To configure the NTP settings, follow these instructions:

1 Click the **NTP** tab.
The page refreshes then displays the NTP Server settings.



Using NTP Server will help you to synchronize the time settings.

Enable NTP: ● Yes ○ No

Enter NTP Server IPs:

Current NTP Status: Not Running

2 To enable NTP, click **Yes**.

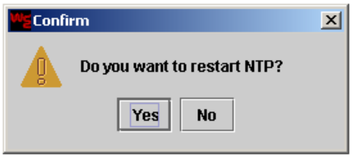
If you later decide to disable NTP, click No.

3 Enter the IP address of an NTP server.

It is possible that the connection to a NTP server can be broken. If this occurs, the Current NTP Status displays “Not Running.”

1 Click **Restart**.

A Confirmation dialog box appears.



Do you want to restart NTP?

2 Click **Yes** to restart NTP.

When you have finished configuring the NTP server settings, click one of the following options:

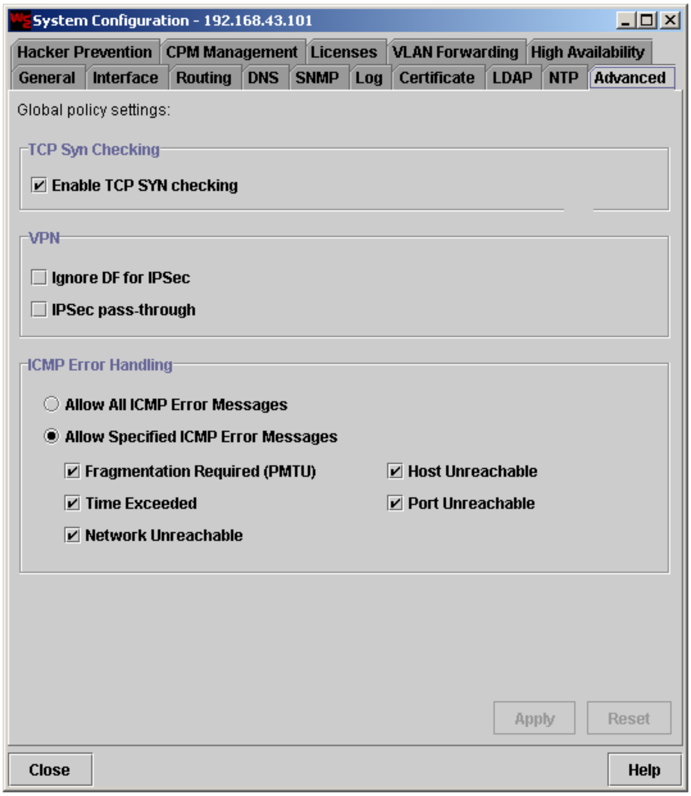
Reset
To return the settings to the previous configuration.

Apply
To immediately commit the settings to the Firebox Vclass appliance.

Advanced Configuration

The **Advanced** tab allows you to configure global policy settings. These settings will apply to all security policies you create. However, you can configure each policy to use a per-policy setting instead of these global settings. For more information regarding the configuration of the advanced settings and security policies, see "Using the Advanced Settings" on page 149.

- Click the **Advanced** tab.
  The Advanced configuration settings are displayed.



Global policy settings:

TCP Syn Checking

☑ Enable TCP SYN checking

VPN

☐ Ignore DF for IPSec

☐ IPSec pass-through

ICMP Error Handling

○ Allow All ICMP Error Messages

● Allow Specified ICMP Error Messages

☑ Fragmentation Required (PMTU) ☑ Host Unreachable

☑ Time Exceeded ☑ Port Unreachable

☑ Network Unreachable

The following global policy settings are displayed:

TCP Syn Checking

This option enables the inspection of a proper TCP three-way handshake. It provides an extra layer of protection against illegal TCP connections.

- To enable TCP SYN checking, click the **Enable Syn Checking** checkbox.

VPN

These options concern the fragmentation of encrypted packets and the ability to allow IPSec users to connect to a different appliance.

- To ignore a DF bit (Don’t Fragment) during an IPSec transmission, click the **Ignore DF for IPSec** checkbox.
- To allow IPSec traffic to pass through to an internal address that is using NAT, click the **IPSec pass-through** checkbox.

ICMP Error Handling

Regular network traffic may include various ICMP error messages. You can allow all of these messages or select the specific messages.

- Select **Allow All ICMP Error Messages** or **Allow Specified ICMP Error Messages**.
- If you selected to allow only specified ICMP error messages, enable the error messages you want to allow.

When you have finished configuring the advanced settings, click one of the following options:

Reset

To return the settings to the previous configuration.

Apply

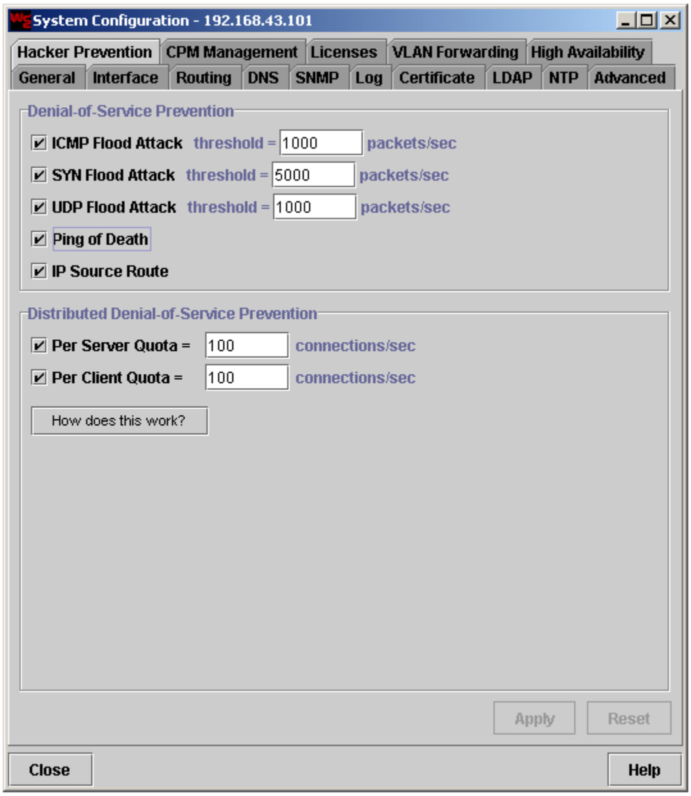
To immediately commit the settings to the Firebox Vclass appliance.

Hacker Prevention Options

If you have not already used the Installation Wizard to set up these options, you can do so now with the **Hacker Prevention** tab’s features. If you have made these entries, you can edit them by using this tab’s features.

1 Click the **Hacker Prevention** tab.

The Hacker Prevention settings are displayed.



Denial-of-Service Prevention

☑ ICMP Flood Attack threshold = 1000 packets/sec

☑ SYN Flood Attack threshold = 5000 packets/sec

☑ UDP Flood Attack threshold = 1000 packets/sec

☑ Ping of Death

☑ IP Source Route

Distributed Denial-of-Service Prevention

☑ Per Server Quota = 100 connections/sec

☑ Per Client Quota = 100 connections/sec

2 You can customize and apply the following two groups of options at this time:

"Denial-of-service" options: These options safeguard your servers from denial-of-service (DOS) attacks. These attacks flood your network with requests for information, clogging servers and possibly shutting down your site. After you activate these options and set threshold numbers, the Firebox Vclass appliance prevents such attacks. If more than the specified number of requests are received (per second), the Firebox Vclass appliance drops the specified excess number of requests within the same second while permitting the specified acceptable number of requests to pass through. This protects your servers from becoming overwhelmed by too many requests within a short period of time.

ICMP Flood Attack

Safeguards your network from a sustained flood of ICMP pings. After clicking the checkbox, enter the threshold number in the text field that will trigger the denial-of-service protection.

SYN Flood Attack

Safeguards your network from a sustained flood of TCP SYN requests without the corresponding ACK response. After clicking the checkbox, enter the threshold number in the text field that will trigger the denial-of-service protection.

UDP Flood Attack

Safeguards your network from a sustained flood of UDP packets. After clicking the checkbox, enter the threshold number in the text field that will trigger the denial-of-service protection.

Ping of Death

Safeguards your network from user-defined large data-packet pings. Click the checkbox to activate this denial-of-service protection.

IP Source Route

Safeguards your network from a flood of false client IP addresses, designed to bypass firewall security. Click the checkbox to activate this denial-of-service protection.

"Distributed Denial-of-service" options: As a subset of denial-of-service attacks, *distributed* DOS attacks occur when hackers coordinate a number of "borrowed" computers for malicious purposes and program them to simultaneously assault a network with information requests. If allowed to pass through, they can overwhelm and crash your Web servers. Your options include the following:

PerServer Quota

Safeguards your servers from coordinated denial-of-service attacks from any client to any single server. After clicking this checkbox, enter a threshold number in the text field that represents the maximum request capacity (per second) of that server. If more than the specified number of connection requests are received within a second, the Firebox Vclass appliance drops the excess requests within that same second. This will protect your server from being overwhelmed by too many connection requests in a short period of time.

Per Client Quota
Restricts the number of connection requests from a single client within a second. After clicking this checkbox, enter a threshold number in the text field that represents the maximum number of requests (per second) from a single client. If more than the specified number of connection requests are received within a second, the Firebox Vclass appliance drops the excess requests within that same second.

When you have finished configuring the Hacker Prevention settings, click one of the following options:

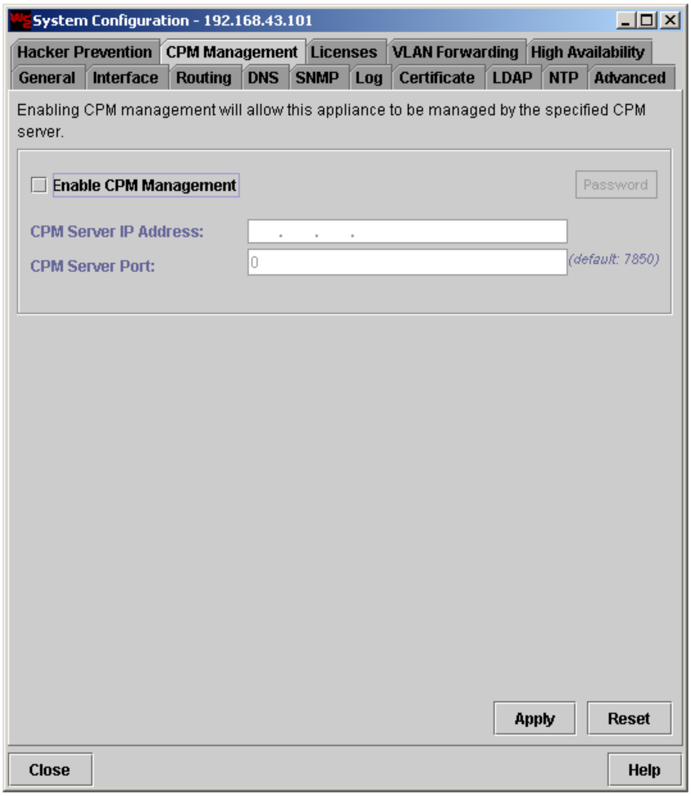
Reset
To return the settings to the previous configuration.

Apply
To immediately commit the settings to the Firebox Vclass appliance.

CPM Management Configuration

Use the **CPM Management** tab to allow a specified CPM server to manage the Firebox Vclass appliance.

1 Click the **CPM Management** tab.
The CPM Management settings are displayed.



Enabling CPM management will allow this appliance to be managed by the specified CPM server.

□ Enable CPM Management

CPM Server IP Address: . . .

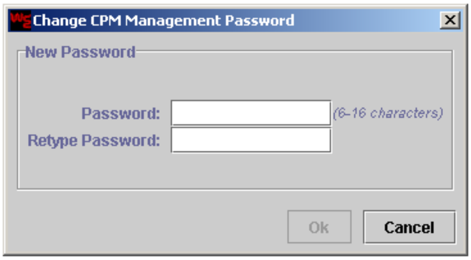
CPM Server Port: 0 (default: 7850)

2 Click the **Enable CPM Management** checkbox.

3 Type the CPM server IP address in the appropriate field.

4 Type the CPM server port in the appropriate field.
The default port is 7850.

5 To change the CPM management password, click **Password**.
The Change CPM Management Password dialog box appears.



Change CPM Management Password

New Password

Password: (6-16 characters)

Retype Password:

6 Type the new password and retype it in the appropriate fields.

7 Click **OK**.

When you have finished configuring the CPM Management settings, click one of the following options:

Reset
To return the settings to the previous configuration.

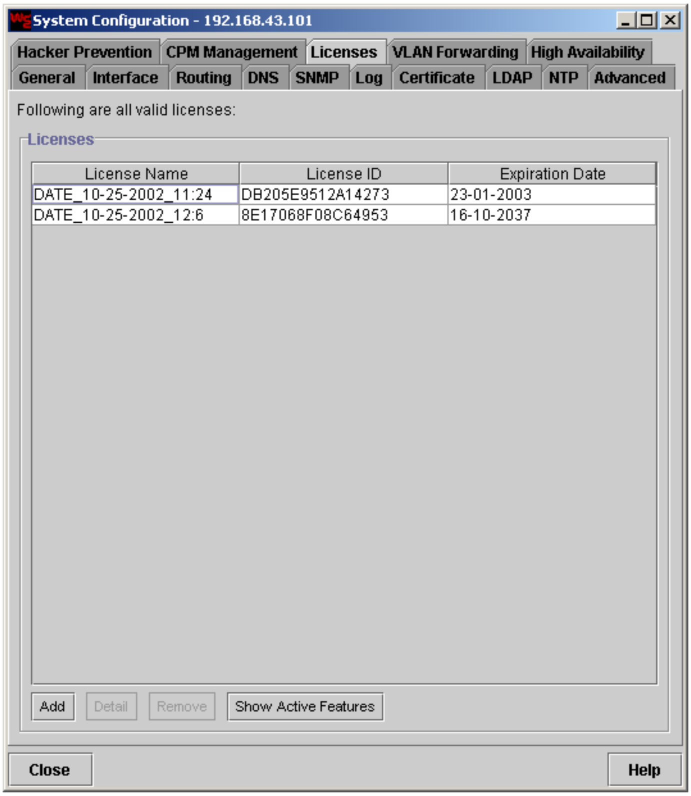
Apply
To immediately commit the settings to the Firebox Vclass appliance.

Managing Software Licenses

Use the **Licenses** tab to import licenses, which you obtain from WatchGuard, and add extra features. For more information about licensing additional features and capacity for your Firebox Vclass appliance, visit the WatchGuard Web site.

To add additional licenses, follow these steps:

1 Click the **License** tab.
The Licences list is displayed.



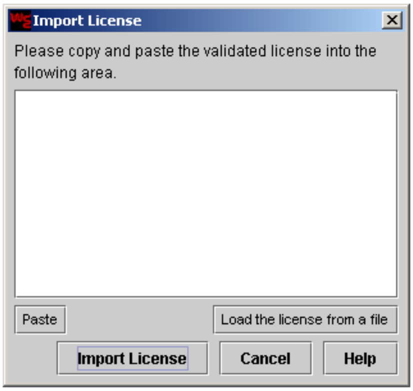
Following are all valid licenses:

License Name	License ID	Expiration Date
DATE_10-25-2002_11:24	DB205E9512A14273	23-01-2003
DATE_10-25-2002_12:6	8E17068F08C64953	16-10-2037

To import a new license, follow these steps:

2 Click **Add**.

The Import License dialog box appears.



Import License

Please copy and paste the validated license into the following area.

3 Click **Load the license from a file**.

4 Locate and select the license file.

NOTE

If you prefer, you can also use a text editor to open the file. Then copy and paste the text.

5 When the license text is displayed, click **Import License**.
This imports the license into the Firebox Vclass appliance. After the import is complete, the dialog box closes and the newly imported license appears in the license list.

6 Repeat this process to import any other certificates into the Firebox Vclass appliance.

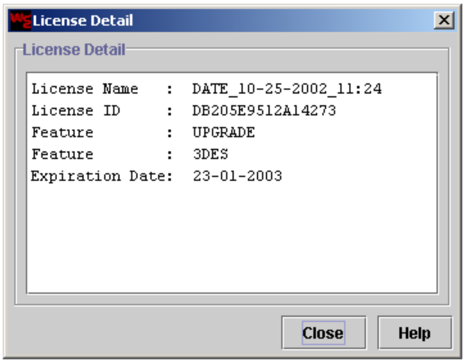
7 To remove a license, select the entry and click **Remove**.
A confirmation dialog box appears.

8 Click **OK**.
The entry is removed from the License list.

To view the details of a particular license, follow these steps:

1 Select an entry from the **Licenses** list.

2 Click Detail.
The License Detail dialog box appears.



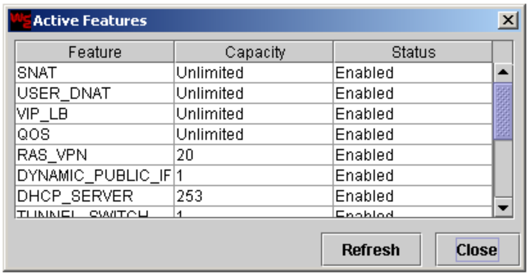
```
License Name   :  DATE_10-25-2002_11:24
License ID     :  DB205E9512A14273
Feature        :  UPGRADE
Feature        :  3DES
Expiration Date:  23-01-2003
```

3 Review the license information.

4 When you are finished, click **Close**.

To see which features are currently active, follow these steps:

1 Click **Show Active Features**.
The Active Features dialog box appears.



Feature	Capacity	Status
SNAT	Unlimited	Enabled
USER_DNAT	Unlimited	Enabled
VIP_LB	Unlimited	Enabled
QOS	Unlimited	Enabled
RAS_VPN	20	Enabled
DYNAMIC_PUBLIC_IF	1	Enabled
DHCP_SERVER	253	Enabled
TUNNEL_SWITCH	1	Enabled

2 Review the active features along with their capacity and status.

3 Click **Refresh** to update the feature list.

4 When you are finished, click **Close**.

VLAN Forwarding Option

Your network may include a number of VLANs. As a result, you may need to create security policies to route traffic between two separate VLANs and this security appliance. In such a situation, which is known as

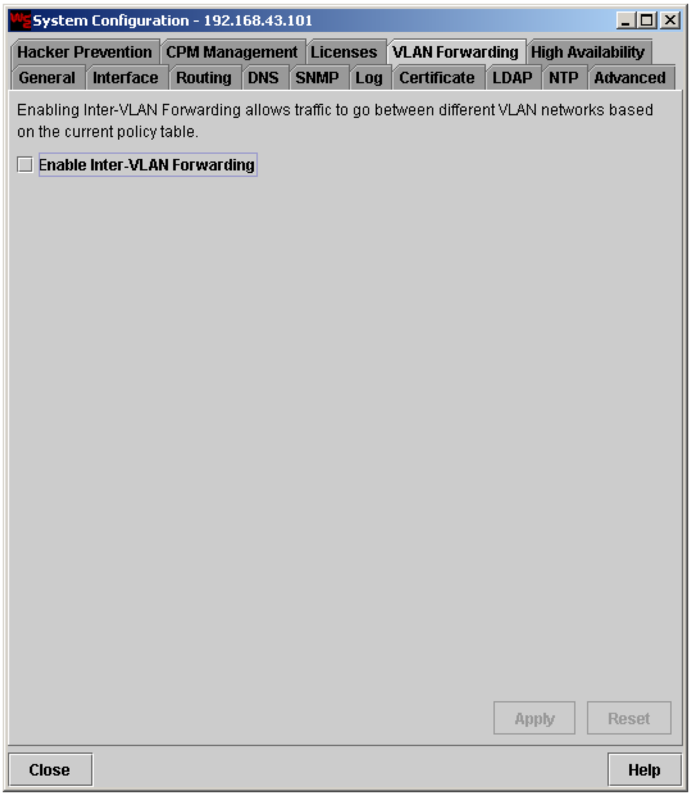
VLAN forwarding, you can create security policies for VLAN traffic, but you must activate the related hardware functionality beforehand, as detailed in this section. This permits the appliance to manage traffic exchanges between two VLANs sharing this appliance, or traffic routed between two VLANs, one using this appliance, and another, separate VLAN behind another appliance, all connected to the same switch.

This function enables you to use an IT management workstation in VLAN 1 to connect through the local gateway appliance and to monitor and maintain a Web server assigned to VLAN 3—which entails inter-VLAN connections.

VLAN forwarding is a feature built into Firebox Vclass appliances, and is inactive by default.

To activate VLAN forwarding, follow these steps:

1 Click the **VLAN Forwarding** tab.
The VLAN Forwarding fields are displayed.



Enabling Inter-VLAN Forwarding allows traffic to go between different VLAN networks based on the current policy table.

□ Enable Inter-VLAN Forwarding

NOTE

If this tab is not visible, this Firebox Vclass appliance does not incorporate these VLAN-forwarding features.

2 Click the checkbox labeled **Activate VLAN Forwarding**.

When you have finished configuring the VLAN Forwarding settings, click one of the following options:

Reset
To return the settings to the previous configuration.

Apply
To immediately commit the settings to the Firebox Vclass appliance.

High Availability Configuration

Use the **High Availability** tab to configure all of the necessary features to connect, link, and run a high-availability system using two HA-ready Firebox Vclass appliances. This provides continuous network management in the event of a security appliance failure.

For complete information on using this tab, see “Setting Up a High Availability System” on page 283.

CHAPTER 6

Using Account Manager

This chapter shows you how to create three separate types of access accounts.

Admin and super admin accounts enable users to connect to a Firebox Vclass appliance so that they can monitor and manage the system. A super admin account grants the user a wide range of controls over the appliance and policies, while the admin account restricts its user to status checks, the policy checker tool, and alarm resolution.

The end user account allows users to connect through a firewall to external networks or the Internet, where such access is blocked by the firewall. It primarily affects internal network users.

Configuring Accounts

Configure system access accounts for any number of users acting in three basic roles.

super admin

This account is given complete control of the entire system. When a user logs into the Vcontroller as a super admin, he or she has access to all the Manager window features and can add to or edit all the settings and policies.

NOTE

Vcontroller provides one default super admin account with primary master privileges. Only one user can be logged in as default super admin at any time, and this connection bars all other secondary super admin account users. See "Account Access Conflicts" on page 111 for more information.

admin

This account is given read-only access to the Vcontroller features, with the exception of the Outstanding Alarms feature. The user of an admin account can open the Vcontroller to check on the status of the system but is not able to change or delete settings. If, however, an alarm is detected, the admin user can log in and both investigate and clear an active alarm. The admin user can also open and use the Policy Checker to help troubleshoot user problems.

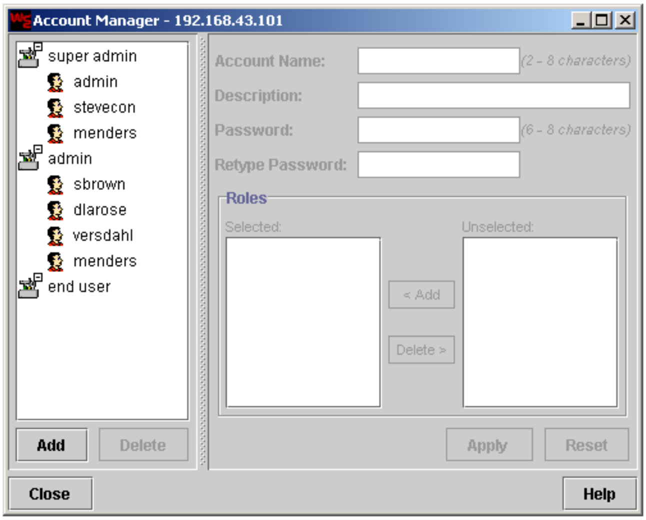
For more information about the prioritization of super admin and admin accounts, see "Account Access Conflicts" on page 111.

end user

This account is related to firewall access and can be used to grant internal users access to external networks or the Internet.

Use the following procedure to configure accounts:

1 From the main Vcontroller page, click **Account**.
The Account Manager dialog box appears.



2 Click **Add**.

The account settings become active.

3 Type an account name in the appropriate field.

The account name must be between 2 and 8 characters.

4 Type a brief description for the account in the **Description** field. This field is optional.

5 Type a password in the appropriate field.

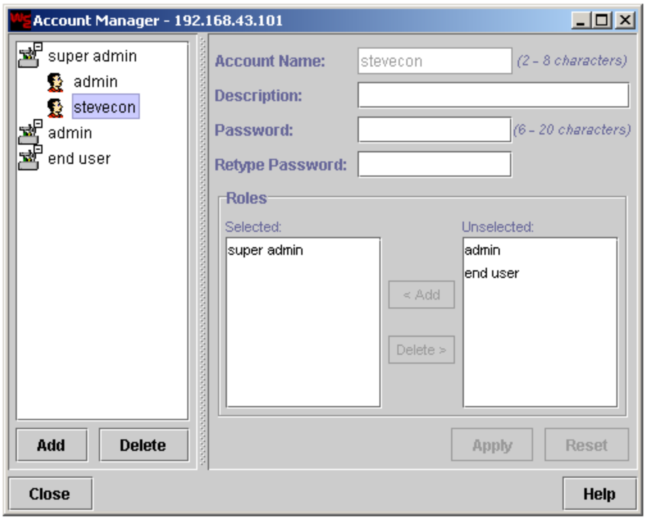
The password must be between 6 and 20 characters.

6 Retype the password in the appropriate field.

7 Select the appropriate role from those displayed in the **Unselected** list. Click **Add** to move the role to the **Selected** column.

8 Click **Apply**.

A new account entry appears below the appropriate user account header on the left.


Account Manager - 192.168.43.101

- super admin
  - admin
  - stevecon
- admin
- end user

Account Name: stevecon (2 - 8 characters)

Description:

Password: (6 - 20 characters)

Retype Password:

Roles

Selected: super admin

Unselected: admin, end user

9 Repeat this process to add more accounts.

10 When you have finished, click **Close**.

End-user accounts for authentication

You can configure a security policy to block internal users from connecting through the Firebox Vclass appliance to the Internet or to other external networks. If, however, a number of inside users need external access, you can grant it to them by creating end-user accounts and configuring a policy to allow authenticated users to bypass the firewall. For more information of creating security policies, see “About Security Policies” on page 113.

Using a Web browser to authenticate

After you have created end-user accounts, contact prospective users and provide them with their end-user account name and password. Communicate the following process for using a Web browser to make a connection.

1 Launch a Web browser.

2 Type the IP address of interface 0 (Private) of the Firebox Vclass appliance as in this example:

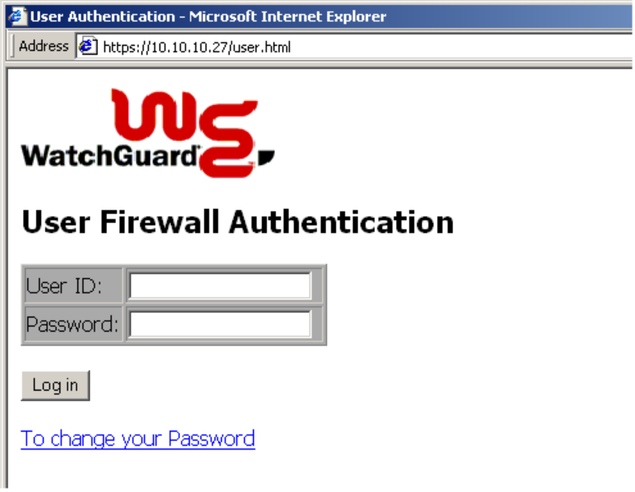
https://10.10.10.27

3 Press **Return**.

A Security Alert dialog box should appear, according to the browser used.

4 Click **Yes/OK** to accept the certificate.

A Login page appears in the Web browser, similar to this example:


User Authentication - Microsoft Internet Explorer
Address
https://10.10.10.27/user.html
WatchGuard
User Firewall Authentication
User ID:
Password:
Log in
To change your Password

5 Type the end-user account name in the **User ID** field.

6 Type the end-user password in the **Password** field.

7 Click **Log In**.

If the entries are accepted, a status message appears in the browser, confirming the connection. The user can now connect to Web sites.

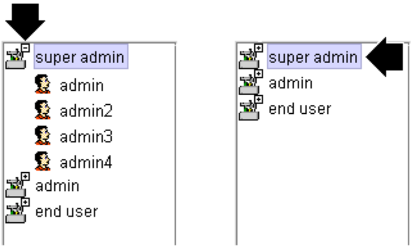
NOTE

All end-user connections have an idle timeout of two hours. If the user does not maintain active connections for two hours, the end-user connection is disconnected, and the end user must log in again.

Managing accounts

Showing and hiding accounts

You can hide accounts in the Account Manager window by double-clicking the minus (–) box at the top of the role mini-icon.



This hides the list of accounts from view, and replaces the minus box with a plus box.

If you need to see all those accounts at a later time, double-click the plus box.

The complete list of accounts appears in the Account Manager window. If needed, you can edit or delete any of the listed accounts, as described in the following sections.

Modifying an existing account

To change an account by adding or removing an access privilege, follow these steps:

1 Open the Account Manager, and expand the category list on the left.

2 Select the account to be edited.
The current access roles of this account appear in the Selected column to the right.

3 To add a new role to this account, select the appropriate role in the **Unselected** column, then click **Add** to move that item into the **Selected** column.

4 To remove a role from this account, select the appropriate role in the **Selected** column, then click **Delete**.

5 When you have finished, click **Apply**.
The Account Manager window displays the results under each of the roles in the left-hand column.

6 Click **Close** to save your entries and quit the Account Manager.

To remove an access account, follow these steps:

1 Determine which account will be deleted. The default super admin account cannot be deleted.

2 Select the account and then click **Delete**.

3 When you have finished, click **Close** to save your changes and close the Account Manager.

External Access for Remote Management

In most instances, you use the Vcontroller to manage a Firebox Vclass appliance through the interface 0 (Private)—this is the default setup and requires the installation of the Vcontroller on a Management Station located on the same private network as the appliance.

In certain settings, a Management Station may be located on a network external from the Firebox Vclass appliance and you must gain external access through interface 1 (Public). To enable remote management, you must create a security policy that allows incoming HTTPS traffic through the interface 1 (Public), while also creating an address group for the IP address of the Management Station. For information on creating a security policy, see “About Security Policies” on page 113.

After a security policy has been configured, you can use an admin account for authentication to the Firebox Vclass just as you would an end-user account. When you have gained external access, you can then use Vcontroller to remotely manage the appliance.

Account Access Conflicts

If you create several super admin access accounts, remember that Firebox Vclass appliances allow only one super admin account to connect at any time with full administrative privileges. If another non-root super admin account user attempts to log in after a root super admin user has already logged in, the second user is granted access to the system, but with admin privileges only.

If someone logs in as a super admin user and a second person then attempts to log in as the default super admin, the second person is given the option of killing (logging out) the first non-default super admin user and taking over full super admin privileges.

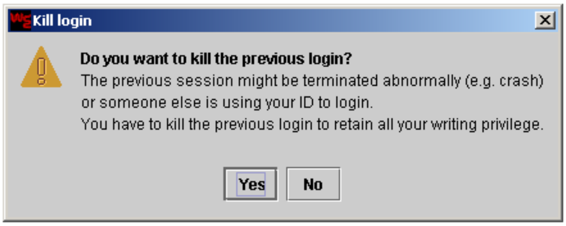
As for all other admin access accounts (which can only be used to check the status and clear new alarms), any number of account users can log in at the same time.

If you attempt to log in as a secondary admin user and the root super admin account is already in use, a warning window appears.

You can still click **OK** to complete the login, but when the Vcontroller appears, you do not have any super admin privileges.

Resolving login conflicts

You can, on occasion, try to log in as the default super admin, and see the **Kill Login** dialog box:



Do you want to kill the previous login?
The previous session might be terminated abnormally (e.g. crash) or someone else is using your ID to login.
You have to kill the previous login to retain all your writing privilege.

This window appears in the following circumstances:

- You were recently logged in as a super admin user and your computer froze or crashed, terminating the administrative session, or you simply exited the Vcontroller and did not log out correctly.
- Another person was already logged in as a non-default super admin user when you attempted to log in with the default super admin account. The appliance gives you the opportunity to quit or to disconnect access for the other user.

You can click **OK** to close a previous session (or to bump a secondary super admin user) and to connect as the root super admin.

When the Vcontroller appears, you have full access to all the features.

CHAPTER 7

About Security Policies

The purpose of a Firebox Vclass appliance is to determine whether data is to be passed or blocked and, if passed, what action will be taken with the data. The set of rules by which data is evaluated and managed is called a *security policy*.

About Security Policies

Every security policy operates in a similar way: it lists qualifications that the Firebox Vclass appliance uses as it analyzes the initial packets of a new stream of data. The sources of data can be your internal network or any external networks including the Internet. Then, if the packets match the traffic specifications of a given policy, the appliance can take several types of actions: firewall actions, IPSec actions (involving manual-key or automatic-key encryption and authentication), a variety of NAT/load-balancing actions, and QoS actions.

You can use Vcontroller to create and combine any number of policies on a Firebox Vclass appliance, enabling that appliance to fully protect and enhance your network traffic.

Security policy components

Every security policy is composed of two basic components: the *traffic specifications* and an *action*.

Traffic specifications

The traffic specification is one of the basic components of a security policy. It defines the source, destination, and other attributes of every data stream traveling through the Firebox.

Traffic specifications incorporate the following components:

Source
Refers to the origin of a stream of data whether it originates in your private network, the DMZ, or an external network.

Destination
Refers to the final destination for traffic that will be passed through the Firebox Vclass appliance by that policy. It can refer to a particular interface.

Service
The type of traffic in this data. For example, HTTP, email, FTP, or Telnet.

Incoming interface
Which interface on the Firebox Vclass appliance the data is coming into: Public, Private, or DMZ.

Tenant
Which tenant is affected, whether a VLAN or user-defined domain tenant.

Policy actions

A policy *action* prompts the Firebox Vclass appliance to perform certain management tasks with data that matches qualifying traffic specifications. Your appliance can take one or more of the following actions:

- Protect your private networks from unauthorized intrusions, if the traffic is external.
- Perform IP address swapping through dynamic and static Network Address Translation.

- Encrypt and authenticate your data for secure transmission through insecure networks.
- Enable various types of load balancing for designated servers.
- Provide various types of network address translation for internal networks.
- Apply Quality of Service (QoS) controls to qualifying data traffic.

You can often combine several actions in the same policy, as described in "Policies with multiple actions" on page 116.

Types of policies

You can use the Vcontroller to create as few or as many policies as are needed by your particular network, with each policy applying one or more compatible actions to qualifying traffic. The range of policies includes the following:

Firewall

Firewall policies block unwanted traffic (including hacker attacks) while permitting valid traffic to proceed to a destination inside your network. You can start with the default firewall policy that blocks every type of traffic, and then insert other policies that permit access by certain types of traffic to specific network destinations.

VPN

Virtual Private Networks create secure tunnels through both internal networks or through the Internet, so that encrypted data can be sent efficiently and securely from one device to the other. VPN policies can be applied to both site-to-site traffic and remote-client-to-site traffic.

Network Address Translation

Network Address Translation (NAT), has three key applications in a Firebox Vclass appliance:

Dynamic Network Address Translation allows you to set up a single IP address so that a large number of internal network users can gain access to the Internet.

S*tatic NAT* policies allow you to substitute an alias IP address for a real IP address. For example, you could mask a Web server IP address behind an alias with SNAT, so that the alias is the only network ID visible to external users.

Virtual IP load balancing uses a single legitimate IP address, and then evenly distributes data requests to any number of servers all mirroring the same information. Your assets are not limited to a single server with a single IP address.

Traffic Shaping

Quality of Service policies assign priorities to qualified data. This can be useful if, for example, an executive wants a particularly fast Web browsing experience. You can create a policy that prioritizes HTTP traffic going to his or her computer's IP address while scaling down the capacity of other traffic.

Hacker Defense

Your Firebox Vclass appliance comes with a suite of options to protect your network against coordinated floods of malicious data requests. You can set threshold values for different types of protection so that the Firebox Vclass appliance automatically dumps the excess traffic and protects your systems from stalling or crashing.

Multi-tenant

You can route VLAN traffic through a Firebox Vclass appliance, including inter-VLAN forwarding, or you can establish a number of user domains to virtually define restricted groups of network tenants and then route traffic to and from the members of that domain.

Scheduling

You can establish hours and days for specific actions that your appliance will take with certain data, while allowing other data to pass unimpeded or unaffected.

Policies with multiple actions

You can combine one or more actions in a policy. For example, suppose you created a VPN policy that permits two server-farm sites to share data with one another. You might also want to implement load balancing, so that the data is distributed equally among several servers. The required policy would focus on the two gateway appliances as source and destination and then apply both an IPSec action and a load-balancing action.

Not all actions can be combined. The following table shows the combinations of actions that can be applied in a single policy.

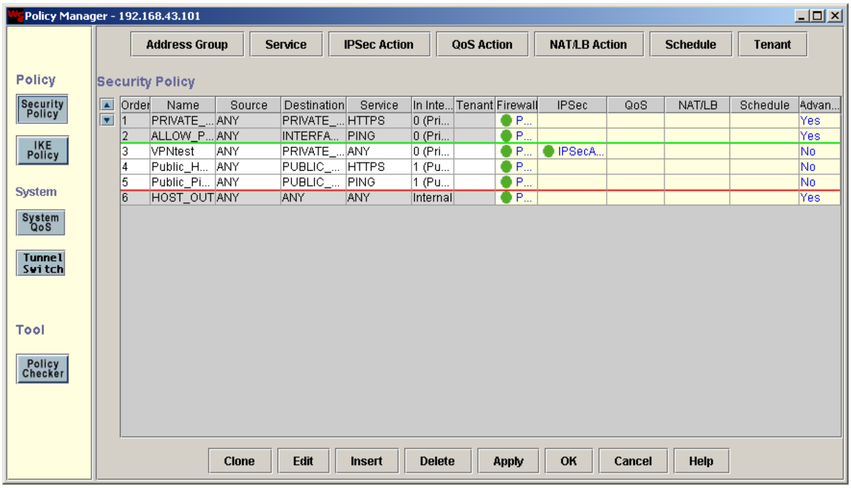
	Firewall	**IPSec**	**Virtual IP/ NAT**	**Dynamic NAT**	**Static NAT**	**QoS**
Firewall	na	YES	YES	YES	YES	YES
IPSec	YES	na	YES	YES	YES	YES
Virtual IP/ NAT[a]	YES	YES	na	NO	NO	YES
Dynamic NAT	YES	YES	NO	na	NO	YES
Static NAT	YES	YES	NO	NO	na	YES
QoS	YES	YES	YES	YES	YES	na

[a]

Using Policy Manager

Policy Manager allows you to create and edit a detailed security policy. Within the security policy, you can create a variety of actions as well as define schedules, address groups, tenants, and other components for security policies. You can also use the Policy Checker to make sure you have defined your policy correctly.

From the main Vcontroller page, click **Security Policy**. The Policy Manager window appears.



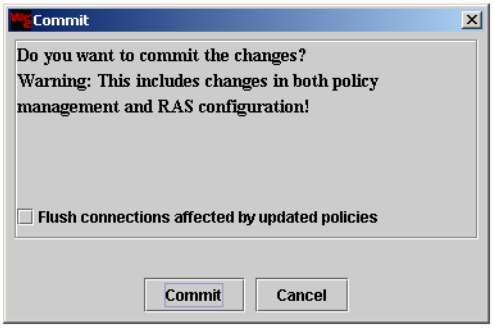
Security Policy

Order	Name	Source	Destination	Service	In Inte...	Tenant	Firewall	IPSec	QoS	NAT/LB	Schedule	Advan...
1	PRIVATE_...	ANY	PRIVATE_...	HTTPS	0 (Pri...		● P...					Yes
2	ALLOW_P...	ANY	INTERFA...	PING	0 (Pri...		● P...					Yes
3	VPNtest	ANY	PRIVATE_...	ANY	0 (Pri...		● P...	● IPSecA...				No
4	Public_H...	ANY	PUBLIC_...	HTTPS	1 (Pu...		● P...					No
5	Public_Pi...	ANY	PUBLIC_...	PING	1 (Pu...		● P...					No
6	HOST_OUT	ANY	ANY	ANY	Internal		● P...					Yes

- Click **Address Group** to view the list of defined entries.
  The Address Group dialog box appears.
  - To create a new Address Group, click **New**. For instructions on defining the entry, see “Defining an address group” on page 126.
  - To edit an address group, select the entry and click **Edit**.
  - To delete an address group, select the entry and click **Delete**.
  - When you are finished, click **Close**.
- Click **Service** to view the list of defined entries.
  The Service dialog box appears.
  - To create a new Service, click **New**. For instructions on defining the entry, see “Defining a service” on page 128.
  - To edit a service, select the entry and click **Edit**.
  - To delete a service, select the entry and click **Delete**.
  - When you are finished, click **Close**.
- Click **IPSec Action** to view the list of defined entries.
  The IPSec Action dialog box appears.
  - To create a new IPSec action, click **New**. For instructions on defining the entry, see “Defining an IPSec action” on page 186.
  - To edit an IPSec action, select the entry and click **Edit**.
  - To delete an IPSec action, select the entry and click **Delete**.
  - When you are finished, click **Close**.

- Click **QoS Action** to view the list of defined entries.
  The QoS Action dialog box appears.
  - To create a new QoS action, click **New**. For instructions on defining the entry, see “Defining a QoS action” on page 138.
  - To edit a QoS action, select the entry and click **Edit**.
  - To delete a QoS action, select the entry and click **Delete**.
  - When you are finished, click **Close**.
- Click **NAT/LB Action** to view the list of defined entries.
  The NAT/LB Action dialog box appears.
  - To create a new NAT or Load Balancing action, click **New**. For instructions on defining the entry, see “About Load Balancing” on page 142.
  - To edit a NAT or Load Balancing action, select the entry and click **Edit**.
  - To delete a NAT or Load Balancing action, select the entry and click **Delete**.
  - When you are finished, click **Close**.
- Click **Schedule** to view the list of defined entries.
  The Schedule dialog box appears.
  - To create a new schedule, click **New**. For instructions on defining the entry, see “Defining a Schedule” on page 147.
  - To edit a schedule, select the entry and click **Edit**.
  - To delete a schedule, select the entry and click **Delete**.
  - When you are finished, click **Close**.
- Click **Tenant** to view the list of defined entries.
  The Tenant dialog box appears.
  - To create a new tenant, click **New**. For instructions on defining the entry, see “Defining tenants” on page 134.
  - To edit a tenant, select the entry and click **Edit**.
  - To delete a tenant, select the entry and click **Delete**.
  - When you are finished, click **Close**.
- To create a duplicate entry, select a policy and click **Clone**.
- To edit a particular entry, select the policy and click **Edit**.
- To delete a particular entry, select the policy and click **Delete**.

- To save the settings to the Management Station and apply them to the Firebox Vclass appliance when it is restarted, click **OK**.
- To close the Policy Manager window without saving or applying any changes, click **Cancel**.
- To immediately commit the settings to the Firebox Vclass appliance, click **Apply**.
  The Commit dialog box appears.



Commit

Do you want to commit the changes?
Warning: This includes changes in both policy management and RAS configuration!

□ Flush connections affected by updated policies

  - To flush any active connections that may be affected by the changes, click the appropriate checkbox and then click **Commit**.
- Click **Help** to launch the online help system within your browser window.
- Click **Security Policy** or **IKE Policy** to toggle between these two displays.

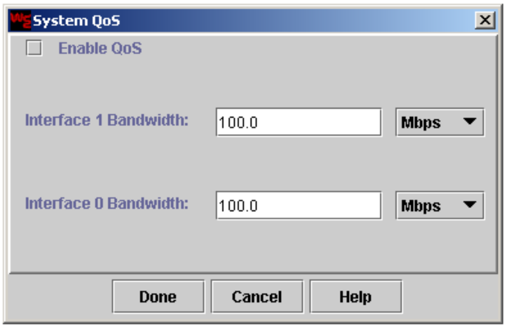
Applying system-wide QoS port shaping

If your Firebox Vclass appliance sends data to a network device—such as a modem, router, or hub—that has a lower throughput speed, you may want to adjust the throughput speed of the Firebox Vclass appliance, so that it does not flood the other device with excessive data. You can set bandwidth constraints for both Private and Public interfaces. This only affects outgoing packets.

This system-wide setting does not directly affect any QoS actions that you may define. Port-shaping settings control overall outgoing throughput, while individual policy actions prioritize specific data.

Follow these steps to apply system-wide QoS port shaping:

1 Click **System QoS**.
The System QoS dialog box appears.



System QoS

☐ Enable QoS

Interface 1 Bandwidth: 100.0 Mbps

Interface 0 Bandwidth: 100.0 Mbps

2 To configure QoS for either the Public or Private interfaces, click the checkbox labeled **Enable QoS**.

3 Select either **Kbps** or **Mbps** from the drop lists.

4 Click **Done**.

Using tunnel switching

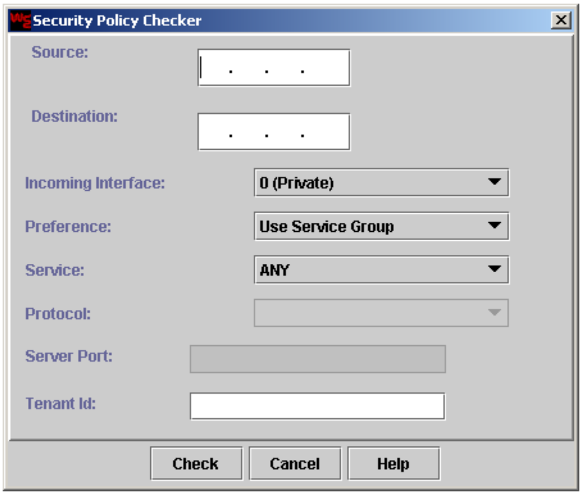
For information on using tunnel switching with VPN policies, see "Using Tunnel Switching" on page 194.

Using Policy Checker

As you compile and insert new policies in the Policy Manager window, you can use the Security Policy Checker window to find and apply the correct policy. This limited test verifies that the policy is in the proper sort order and that it will be activated when qualifying data is detected.

Follow these steps to test a security policy:

1 Click **Policy Checker**.
The Security Policy Checker dialog box appears.



Security Policy Checker

Source: . . .

Destination: . . .

Incoming Interface: 0 (Private)

Preference: Use Service Group

Service: ANY

Protocol:

Server Port:

Tenant Id:

2. Type the IP address of the external device from which the expected source traffic will arrive in the **Source** field.
3. Type the IP address of the internal device to which the expected source traffic will arrive in the **Destination** field.
4. Select the appropriate interface at which the expected traffic will arrive from the **Incoming Interface** drop list.
5. From the **Preference** drop list, select one of the following:

   Use Service Group

   If you select this item, the **Service** drop list is your only active option.

   Use Protocol and Port

   If you select this item, the Protocol and Service Port features become active (and the Service drop list becomes inactive.)

6. From the **Service** drop list (if active), select the service this policy should check for.
7. From the **Protocol** drop list (if active), select the protocol to be used.
8. In the **Server Port** field (if active), type the port number for this protocol.
9. Enter the **Tenant ID**, if this test will verify a policy for multi-tenant domain traffic.
10. Click **Done**.

The Policy Checker starts at the top of the policy list and checks your test parameters against every rule. If it finds a match, the first policy affected by such traffic is highlighted in the Policy Manager list. This is particularly helpful when you have a long list of policies and you want to:

- Change the order of policies.
- Edit each policy to change any overlapping settings

If no match is found, either your newly created policy contained errors, or the test scenario you hoped to validate had errors in the settings. To examine the rule and its settings, follow these steps:

1. Resort the policies in the window and use the Security Policy Checker again to test the sort order (after verifying your test traffic entries).
2. If no matching policy is found, select the policy that should have been applied to the test traffic, and double-click **Edit**.
   The Edit Security Policy dialog box appears.
3. Because this dialog box has the same features as the **Insert Security Policy** dialog box, you can check all the configuration options, drop lists, text fields, and checkboxes to find the incorrect entry.
4. After you are finished, reopen the Security Policy Checker dialog box, re-enter the test scenario settings, and try again.

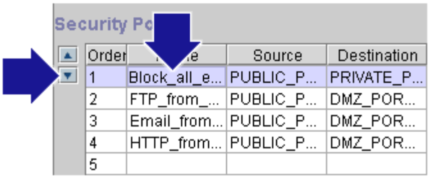
How policy order governs policy application

Vcontroller applies policies to new data in the order you set. This order can be critical to the proper operation of your Firebox Vclass appliance. For example, suppose you define a policy that admits HTTP packet streams, and you list this policy second in order. However, suppose the first policy in the list blocks all HTTP traffic from entry. Because the first policy blocks all HTTP traffic, the second policy is not applied.

Because policies can make use of wildcards or nested address groups, make sure you define and list all of your policy rules in the proper order.

After you have created a number of policies and tested them, you may need to move one or more policies out of their current place to another, to permit them to be used before or after other existing policies. To do this, use the arrow buttons to the left of the policy list in the Policy Manager window.

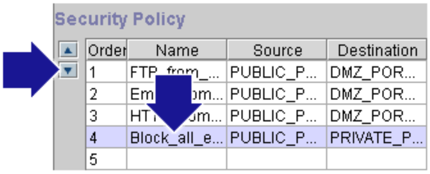
- Select the policy to be moved, as shown below in row 1.



Security Po

Order	e	Source	Destination
1	Block_all_e...	PUBLIC_P...	PRIVATE_P...
2	FTP_from_...	PUBLIC_P...	DMZ_POR...
3	Email_from...	PUBLIC_P...	DMZ_POR...
4	HTTP_from...	PUBLIC_P...	DMZ_POR...
5			

- Click the **Up** or **Down** arrow key, as shown above, depending on which direction the move is to occur.
- Continue to click until the selected policy appears in the desired location, as shown here. This illustration shows the selected policy has been moved from row 1 to row 4.



Security Policy

Order	Name	Source	Destination
1	FTP_from_...	PUBLIC_P...	DMZ_POR...
2	Em om...	PUBLIC_P...	DMZ_POR...
3	HT om...	PUBLIC_P...	DMZ_POR...
4	Block_all_e...	PUBLIC_P...	PRIVATE_P...
5			

Default policies

When you first install the Vcontroller, three preinstalled policies are put into effect.

PRIVATE_HTTPS

Permits incoming HTTPS traffic access to interface 0 (Private). Vcontroller uses HTTPS traffic, so this policy allows management connections to the private interface.

Allow_PING_FROM_PVT

Permits you to ping interface 0 (Private). This allows you to troubleshoot your connection to the private interface.

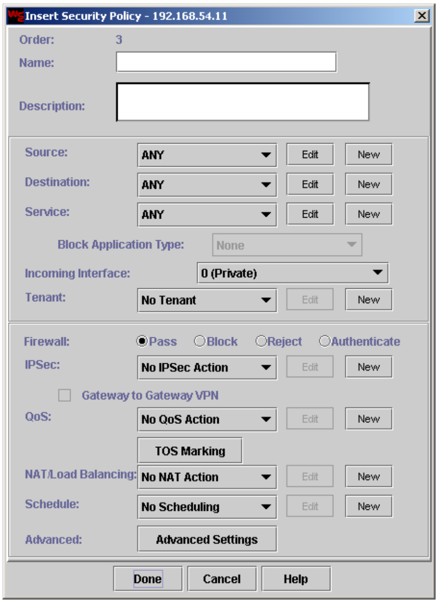
HOST_OUT

Permits all outgoing traffic, regardless from which internal interface the traffic originates, access to external networks such as the Internet.

Defining a Security Policy

The **Insert Security Policy** dialog box allows you to combine traffic specifications and policy actions. You use this dialog box to define all security policies regardless of type.

Select an entry point among the list of policies and then click **Insert**. The **Insert Security Policy** dialog box appears.



Insert Security Policy - 192.168.54.11

Order: 3

Name:

Description:

Source: ANY

Destination: ANY

Service: ANY

Block Application Type: None

Incoming Interface: 0 (Private)

Tenant: No Tenant

Firewall: ● Pass ○ Block ○ Reject ○ Authenticate

IPSec: No IPSec Action

□ Gateway to Gateway VPN

QoS: No QoS Action

NAT/Load Balancing: No NAT Action

Schedule: No Scheduling

Advanced:

Defining source and destination

The default sources and destinations are as follows:

ANY
This represents any possible source or destination. It is useful when selecting sources or destinations outside your network.

PRIVATE_PORT_IP
The IP address of the Private interface.

PUBLIC _PORT_IP
The IP address of the Public interface.

DMZ_PORT_IP
The IP address of the DMZ interface.

DMZ2_PORT_IP
The IP address of the second DMZ interface.

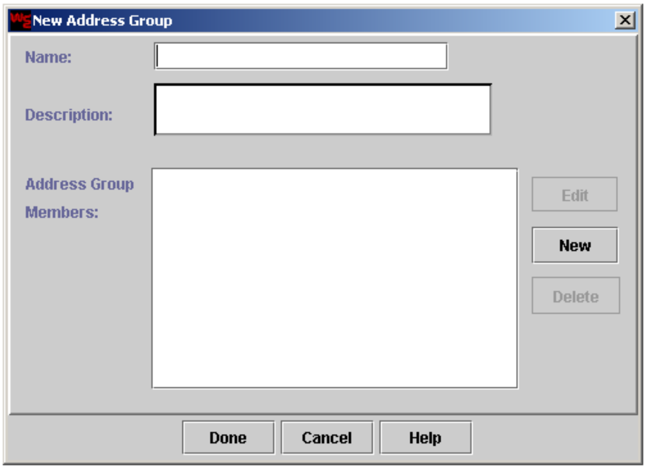
INTERFACE_IPS
The IP addresses of all interfaces.

If none of the listed items represent the source or destination you want to use for a policy, you must define a new address group, as described in the next section.

Defining an address group

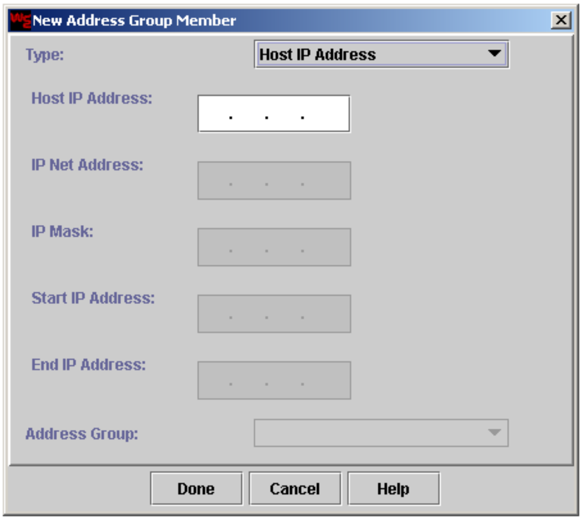
Follow these steps to define an address group:

1 Click **New**, next to the **Source** or **Destination** drop list.
The New Address Group dialog box appears.



2 Type a name and brief description for the address group in the appropriate fields. The **Description** field is optional.

3 Click **New**.
The New Address Group Member window appears.



Type: Host IP Address

4 From the **Type** drop list, select the category of members that will be the source or destination of traffic. The options include the following:

Host IP Address
A single host (or a single networked device).

IP Network Address
A particular subnet.

IP Address Range
A series of sequentially numbered IP addresses.

Address Group
An existing address group.

5 If you chose **Host IP Address**, in the **Host IP Address** text field, type the host computer's IP address.

If you chose **IP Network Address**, type the subnet address and subnet mask for this network.

If you chose **IP Address Range**, type the starting and ending IP addresses for the range.

If you chose **Address Group**, from the **Address Group** drop list, select the appropriate item. This drop list lists every address group created for use with the Firebox Vclass appliance.

6 When you are finished, click **Done**.

The new member name is displayed in the Address Group Members list of the New Address Group dialog box.

7 Repeat this process until you have defined all the required members.

8 After you have added all the required group members, click **Done** to close the **New Address Group** dialog box.

When the Insert New Policy dialog box reappears, the Source or Destination drop list automatically displays the newly created address group.

NOTE

You can nest address groups as "members" within other address groups, as suggested by the Address Group drop list in the New Address Group Member dialog box. This does require, however, the creation of each group before you can do so. For example, you could create an address group representing employee departments or employees within a subnet, then, in a separate process, create a master address group, "Employees," that contains, as members, all the other staff address groups.

Defining a service

The service component of a traffic specification enables you to designate one or more network protocols that will be used by the source device for a particular data stream. Your service selection will be a *service group*, which can consist of any combination of the following attributes:

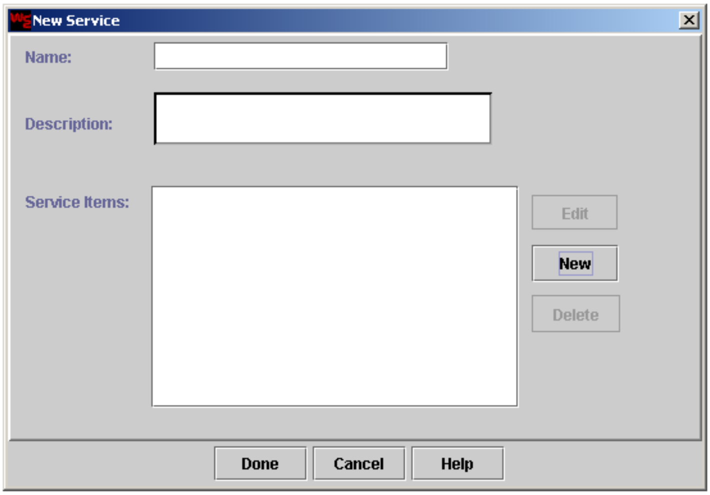
- A single service for a particular type of data traffic, which includes a single protocol and port number.
- A range of port numbers used by a single service or application.
- An existing service group, which includes two more related services.

You can assemble a service group of one or more services for use in a single policy to save you from having to create a separate policy for each service. Although a comprehensive set of protocols is included in the **Service** drop list, you can create a new service group using the procedure in the next section.

Follow these steps to create a new service group:

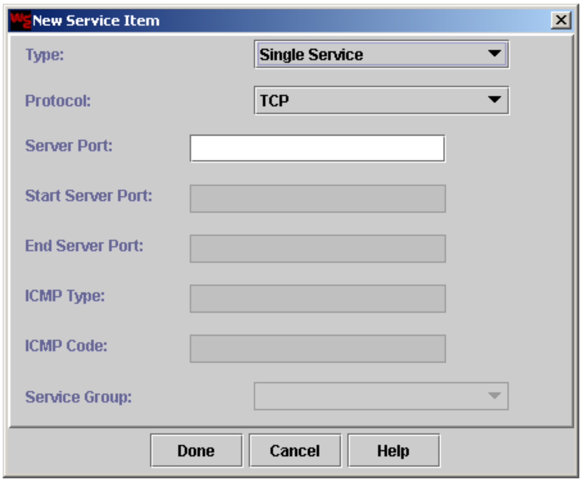
1 Click **New**, next to the **Service** drop list.

The New Service dialog box appears.



2 Type a name and brief description for the service in the appropriate fields. The **Description** field is optional.

3 Click **New**.
The New Service Item dialog box appears.


Type: Single Service

Protocol: TCP

4 From the **Type** drop list, select the appropriate option.

5 To create a service group combining a protocol and port number, follow these steps:

- Select **Single Service** from the **Type** drop list.
- From the **Protocol** drop list, make the appropriate selection.
- In the **Server Port** field, type the port number used by this protocol.
- Click **Done**.

6 To create a service group containing a single protocol and a range of port numbers, follow these steps:
   - Select **Service Range** from the **Type** drop list.
   - From the **Protocol** drop list, make the appropriate selection.
   - In the **Start Server Port** field, type the lowest port number used by this protocol.
   - In the **End Server Port** field, type the highest port number.
   - Click **Done**.

7 To combine two or more existing services into a convenient group, follow these steps:
   - Select **Service Group** from the **Type** drop list.
   - From the **Protocol** drop list, select the first service you want to add to this group.
   - The **New Service** dialog box reappears, listing your new service group.
   - Click **New**, and repeat the **Type** and **Service Group** selection process to add another service to this group.
   - Repeat this process until all your intended services appear in the Service Items list in the **Service Items** field.

8 When the group is complete, click **Done**.
When the Insert Security Policy dialog box reappears, the Service drop list automatically displays this new group as your selection.

NOTE

If this group is for use in a policy that blocks traffic of some type, remember that blocking a service group effectively blocks all the service items in that group. Before doing so, you must make sure this is indeed your intent. You'll only rarely need to block an entire service group; instead, you should block only the relevant service items.

Defining the incoming interface

The final component of a traffic specification is the *incoming interface*, which represents the actual Ethernet interface at which data packets are detected by the Firebox Vclass appliance. The choices for the incoming interface are as follows:

0 (Private)
Also considered the “trusted” interface. This interface receives traffic originating from your internal networks.

1 (Public)
Also considered the “external” interface. This interface receives traffic originating from external networks, such as the Internet.

2 (DMZ)
Also considered an “optional” interface. This interface receives traffic originating from both external networks as well as your internal networks. This interface is not available on the V10 or V100 models.

3 (DMZ2)
Also considered an “optional” interface. This interface receives traffic originating from both external networks as well as your internal networks. This interface is not available on the V10 or V100 models.

Internal
The traffic originates from within the appliance itself. For example, you would use this option if you created a policy that permits RADIUS query traffic to go to a VLAN network.

Using Tenants

Using Vcontroller, you can create policies that direct traffic in a multi-tenant network environment. Generally used in a service provider environment, a customer’s tenant assets are segregated into separate Virtual LANs (VLANs). This provides a secured environment for tenants because all network traffic between different VLANs is separated by VLAN switches.

All Vclass security appliances support IEEE 802.1q VLAN packets, which allows a network administrator to create separate policies for each tenant using a single shared security appliance. This reduces the cost of providing firewall and VPN services to all tenants.

In addition to VLAN-type tenants, all Vclass security appliances allow administrators to apply security policies to VLAN-like tenants in a non-VLAN environment. This type of tenancy is called a *user domain*. By logging on and providing a user ID, password, and domain name to a Vclass security appliance, an end user can access the Internet or use VPN policies defined for his or her specified domain. Creating user-domain tenant policies is an easy way to achieve multi-tenant application without the need for VLAN hardware. This is especially useful when tenants cannot be distinguished by different IP subnets.

About VLANs and tenants

VLANs have become increasingly popular for both corporate networks and service providers as a way of partitioning a network into discrete regions. VLANs can also be used to segregate a number of users who need to remain separate from one another.

The Firebox Vclass appliance permits you to use VLAN tags or IDs as part of the traffic specification in a policy, so that your appliance can route traffic to and from a VLAN segment by means of a VLAN switch. This permits bidirectional traffic from the VLAN segment to other segments, network regions, or to the Internet.

To assist network administrators in creating security policies for use in a VLAN-enabled environment, the Vcontroller allows definitions of *VLAN tenants*, which can be used as part of the traffic specification in security policies. The VLAN tenant entry represents the VLAN ID embedded in a data stream packet that will be used by the VLAN switch.

Conceptually, security policies that incorporate the same VLAN object will be grouped into the same policy domain. Although Vcontroller does not require all policies with the same VLAN object to be grouped together in the Policy Manager security policy table, WatchGuard recommends that you do so for better policy management.

NOTE

The current line of Firebox Vclass appliances recognize VLAN/802.1Q headers in data for routing purposes.

User domain tenant authentication

Two types of tenant authentication can be applied in a user domain multitenant policy:

Manual authentication

The client user supplies three required entries by means of a Web browser form: a user name, a password, and a domain name.

Certificate-based authentication

A pre-installed VPN certificate automatically supplies the client user name and domain name. The password must be manually entered by the user. This certificate must be imported by an IT administrator into the client system's Web browser (which is required for all secure access).

After the three entries are supplied to the Firebox Vclass appliance, the appliance initiates a RADIUS system authentication request to check the user name and password. Note, however, that Firebox Vclass appliances cannot perform tenant authentication because they have no database for this purpose.

After a user domain tenancy is established for relevant users, and the RADIUS system is loaded with authentication data for the potential users, the actual network connections are managed in this manner:

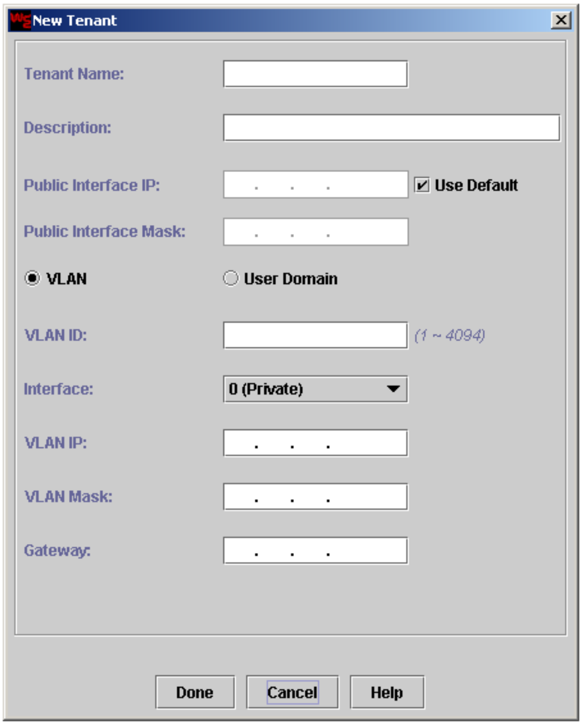
- The user opens his or her browser and attempts to connect to the Firebox Vclass appliance.
- When the connection is made, a Login form appears in the browser.
- The user clicks in each of the three text entry fields and types the required information.
- The browser displays either a Confirmation message, indicating that the connection is complete and ready for use, or an Invalid Entry alert, allowing the user to try reentering his or her login information.
- The user can now perform any network tasks with this connection.

Defining tenants

Follow these steps to create VLAN tenants:

1 Click **New** next to the **Tenant** drop list.

The New Tenant dialog box appears.



New Tenant

Tenant Name:

Description:

Public Interface IP: . . . ☑ Use Default

Public Interface Mask: . . .

● VLAN ○ User Domain

VLAN ID: (1 ~ 4094)

Interface: 0 (Private)

VLAN IP: . . .

VLAN Mask: . . .

Gateway: . . .

2 Type a name and brief description for the tenant in the appropriate fields. The **Description** field is optional.

3 Type the IP address and netmask of the public interface in the appropriate field, or click **Use Default** to use the default IP address and netmask.

4 Enable either the **VLAN** or **User Domain** option.

The dialog box refreshes and fields are displayed relevant to the VLAN or User Domain option enabled.

Follow these steps to configure the VLAN option:

1 Type the pre-assigned number (between 1 and 4094) that will identify this VLAN traffic in the **VLAN ID** field.

2 Select the interface that connects to the VLAN network from the **Interface** drop list.

3 In the **VLAN IP** field, type the IP address that is assigned to the interface on the specified VLAN network.

This IP address can also be used as a default gateway address for the devices on the specified VLAN network.

4 In the **VLAN Mask** field, type the mask associated with the VLAN IP address.

5 In the **Gateway** field, type the gateway address for traffic going to the specified VLAN network.

This entry must be in the same subnet as defined by the VLAN IP address and subnet mask.

6 Click **Done**.

7 Repeat this process as needed to create additional VLAN tenant entries.

Follow these steps to configure the User Domain option:

1 In the **Tenant ID** field, type a number (5001 or higher) to identify this particular tenant's traffic.

2 In the **Idle Time Out** field, type the number of minutes a tenant user's connection can remain idle before it is automatically terminated.

3 In the **RADIUS IP** field, type the IP address of the RADIUS server.

4 In the **RADIUS Secret** field, type the password used by this Firebox to gain access to the RADIUS system. In the **Confirm Secret** field, retype the same RADIUS password.

5 If the RADIUS server is not using the default UDP port (shown in the **RADIUS Port** field), click to clear the checkbox labeled **Use Default**. In the **RADIUS Port** field, type the correct port number.

6 In the **Request Time Out** field, type the number of seconds that determine when an unanswered authentication request to the RADIUS system will be dropped. Two seconds is the recommended value.

7 In the **Request Retry** field, type the number of retries that this appliance will make in requesting authentication from the RADIUS system if the initial attempts go unanswered.

8 In the **Secondary RADIUS IP** field, type the IP address of any available backup RADIUS server. This step is optional.

9. In the **Secondary RADIUS Secret** field, type the password used by this Firebox to gain access to any available backup RADIUS system. In the **Confirm Secret** field, retype the same RADIUS password. This step is optional.
10. If the Secondary RADIUS server is not using the default UDP port (shown in the **Backup RADIUS Port** field), click to clear the checkbox marked **Use Default**. In the **Backup RADIUS Port** field, type the correct port number. This step is optional.
11. Click **Done**.
12. Repeat the process as needed to additional user-domain tenants.

Using the Firewall Options

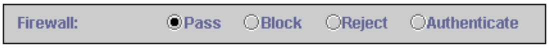
A Firebox Vclass security appliance protects network assets by means of a *firewall policy*. This type of policy blocks unwanted traffic while permitting valid traffic to enter your network. For example, you can define a firewall policy to block all types of service requests, such as FTP, while permitting authorized external traffic to a group of servers connected to interface 2 (DMZ).

You can define multiple firewall policies to work in conjunction with each other. For example, in addition to the policy described previously, you could define a separate policy that grants HTTP access to the Internet for internal users.

You can also define a firewall policy for internal traffic, to block internal network users from unauthorized Internet access, such as Web browsing.

Defining the firewall action

The firewall action is defined in the section directly below the traffic specifications, as shown in the following figure. Select one of the following options to define what you want the firewall to do with the traffic defined by the traffic specification.



Firewall: ● Pass ○ Block ○ Reject ○ Authenticate

Pass

Permits all qualifying external traffic through the firewall.

Block

Prevents all qualifying traffic from gaining access to your network.

Reject

Blocks incoming traffic from the source and sends a TCP reset message back to that source's interface.

Authenticate

Requires that internal users authenticate to the Firebox Vclass appliance before they are granted access through the firewall to external networks.

If you select the **Authenticate** option, you must create end user accounts for use by authorized users. For more instructions on using the **Authenticate** option, see "End-user accounts for authentication" on page 108.

Using Quality of Service (QoS)

In an extensive network with a large number of host computers, the volume of data moving through the Internet can be immense. When the traffic is more than the network can sustain, data packets are simply dropped as a result of congestion. In short, the network does not have enough bandwidth to deliver all the traffic when it enters the network. When severe network congestion occurs, all traffic is affected equally.

The Firebox Vclass security appliance offers two Quality-of-Service (QoS) features that enable you to assign more bandwidth to your most valuable traffic.

The QoS features implemented in Firebox Vclass appliances include Weighted Fair Queuing (WFQ), Type of Service (TOS) marking, and port shaping.

The WFQ algorithm

This data queueing technique allows you to assign a relative bandwidth ratio for specific types of traffic with different weights.

For example, data exchanges between the corporate center and branch offices can be allotted a weight of 20 while Internet traffic is given a weight of 4. During periods of extreme network congestion, the traffic between HQ and branch offices will benefit from five times more bandwidth than that allowed to outbound Internet data.

TOS marking

This allows you to overwrite the TOS byte value in the IP header of qualified packets. These TOS values can be used by routers that recognize *TOS precedence/DTR bits* or by routers that implement *Differentiate Services Code Point* (DCP) so that they can prioritize packets during routing.

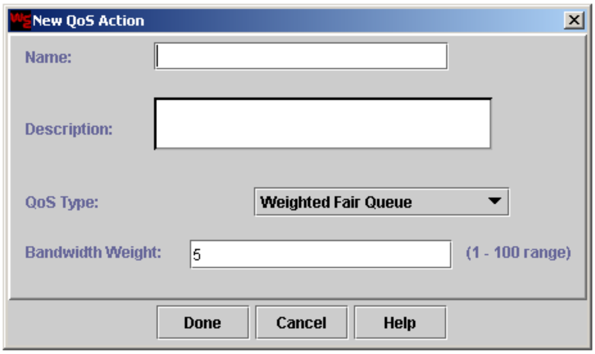
Port shaping

This allows you to restrict the bandwidth of outgoing traffic directed through interface 0 or interface 1. Typically, interface 0 is connected to the private network with higher capacity connections than interface 1, which is usually connected to the Internet through a lower-capacity T1 line. In such a case, packets in outgoing traffic are dropped due to the physical limitations of the internal-to-external connection. With port shaping, you can restrict the overall capacity of interface 1 to match the actual bandwidth of the physical connection. If a huge volume of traffic comes from the private network to interface 1, packets are transmitted according to the weight defined in a QoS policy action—with no unnecessary loss of packets.

Defining a QoS action

Follow these steps to define a QoS action:

1 Click **New**, next to the **QoS Action** drop list.
The New QoS Action dialog box appears.



QoS Type: Weighted Fair Queue

Bandwidth Weight: 5 (1 - 100 range)

2 Type a name and brief description for the QoS action in the appropriate fields. The **Description** field is optional.

3 From the **QoS Type** drop list, select **Weighted Fair Queue**. This is the only selection available at this time.

4 In the **Bandwidth Weight** field, type the percentage of bandwidth you want to assign to qualifying data.

You can type a value ranging from 1 to 100. Note that traffic with a weight of 20 will be given five times more bandwidth than traffic with weight of 4 during periods of network congestion.

5 Click **Done**.

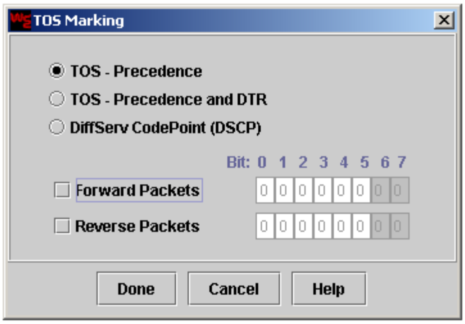
Activating TOS marking

You can now activate and customize the TOS Marking values, which enables this policy to overwrite the TOS byte in the IP header of qualified incoming packets. Before doing so, make sure you know the direction of traffic that will be affected by this policy, so you can determine whether marking will be forward, reverse, or both.

Follow these steps to activate TOS marking:

1 Click **TOS Marking**.

The TOS Marking dialog box appears.



TOS Marking

● TOS - Precedence

○ TOS - Precedence and DTR

○ DiffServ CodePoint (DSCP)

	Bit:	0	1	2	3	4	5	6	7
□ Forward Packets		0	0	0	0	0	0	0	0
□ Reverse Packets		0	0	0	0	0	0	0	0

2 Click one of the following TOS marking options: **TOS Precedence**, **TOS Precedence and DTR**, or **DiffServe CodePoint**.

3 Enable either **Forward**, **Reverse**, or both.

Forward
The policy will mark the packets that are transmitted in the same direction as this policy.

Reverse
The policy will mark packets sent in the reverse direction of this policy.

4 Depending on your TOS choice, a number of **Bit** fields become active. If **TOS Precedence** is your choice, the first three fields (0, 1, and 2) become active. If you selected either of the remaining TOS options, the first six fields—0 through 5—become active.

To toggle a particular field's bit to ON, click the 0 in a field, which will automatically turn into a 1. To reverse this setting, click the 1 to restore it to 0.

5 Click **Done**.

About NAT

Network address translation (NAT) takes IP addresses used on one network and translates them into IP addresses used within another network. Also called IP masquerading or port forwarding, you use NAT to hide network addresses from hosts on another network. Hosts elsewhere only see outgoing packets from the Firebox Vclass appliance itself. You can improve security by mapping inside (private or trusted) addresses to outside (public or optional) addresses. Using NAT also conserves the number of global IP addresses your company needs. More importantly, with NAT you can use a single public IP address for all outgoing and incoming communication, which keeps your trusted addresses secure.

Static NAT

You may have situations in which you want a subnet, a server, or a group of users to be associated with a different IP address than the one actually assigned to them. Whether you want to maintain privacy for a number of client users or hide internal assets from external view, you can do so with static network address translation (*static NAT*).

The most important parameters necessary for creation of a static NAT policy are:

- The internal IP address of the private network asset/client
- The external IP address to which this internal device's IP address will be mapped

You can apply one-to-one, many-to-many, or subnet-to-subnet static NAT policies to qualifying traffic. All types of static NAT action are described in this section.

Before you proceed, you should be aware of the following constraints on static NAT policies as applied by a Firebox Vclass appliance:

- Static NAT policies are limited in that they can translate only IP addresses.
- Static NAT policies do not support VIP load balancing.
- If a VPN policy includes a static NAT action, the peer tunnel IP address cited in the IPSec action must be the primary interface 0 IP address, not any of the secondary addresses assigned to this interface.
- If IP addresses that are to be mapped are not in the same subnet as interface 1 (Public), proper routing must be configured to ensure that traffic to these mapped IP addresses is routed to interface 1 of this appliance.

Dynamic NAT

If you have a number of employees or other private network users whose client computers have been assigned IP addresses for internal use, you can grant all of them full access to the Internet using dynamic Network Address Translation (*dynamic NAT*).

You can insert policies into a Firebox Vclass security appliance that apply dynamic NAT to qualified traffic in the following ways:

Public IP
This action substitutes the IP address of the 0 *(Public)* interface on the appliance for all internal use IP addresses. This allows internal users to gain one-way access to the Internet using the IP address of the appliance's Public interface.

User assigned IP
This action substitutes a publicly routable IP address of your choosing for internal use IP addresses. This option is particularly useful if this appliance will be managing more than 55,000 simultaneous sessions using the IP address of the Public interface.

About Load Balancing

As an efficient traffic management scheme, *load balancing* enables you to distribute incoming data requests to an array of servers. Additionally, you can fine-tune the distribution, directing a percentage of the overall traffic to specific servers according to the capacity of those devices. With the Vcontroller and a security appliance, you can create a policy that lists each server, and then assigns a percentage of total requests to that server (based on its capacity in comparison to other servers). After you apply this policy to your network traffic, your Firebox Vclass security appliance distributes new data requests to additional servers in the queue after previous servers have been fully utilized.

Load balancing also makes use of a virtual IP address (a form of dynamic Network Address Translation), to which all requests are directed, and through which the security appliance will distribute the overall load. All load balancing policies must use the Public interface of the Firebox Vclass appliance.

Defining a NAT Action

To create a Dynamic NAT action using a Public IP address:

- Select Dynamic NAT from the **NAT/Load Balancing** drop list. This automatically establishes the IP address of interface 1 (Public) of the Firebox Vclass appliance as the translation address.

Follow these steps to create a Dynamic NAT action using a user-defined IP address:

1 Select either 0 (Private), 2 (DMZ), or 3 (DMZ2) from the **Incoming Interface** drop list.

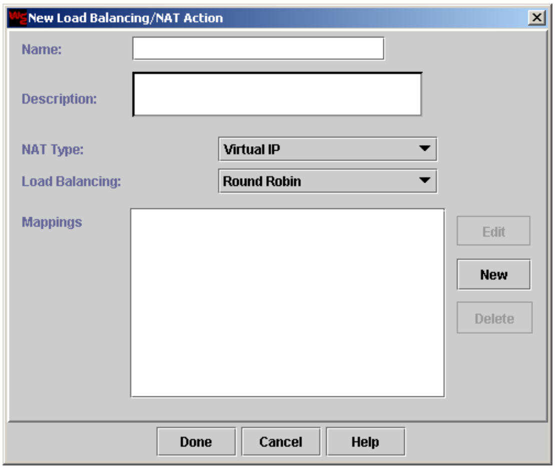
You cannot apply dynamic NAT to interface 1 (Private).

2 If a VLAN or user domain tenant is affected by this action, select the appropriate entry from the **Tenant** drop list.

3 Select **Dynamic NAT** from the **NAT/Load Balancing** drop list.

4 Click **New** from the right of the **NAT/Load Balancing** drop list.

The New Load Balancing/NAT Action dialog box appears.



New Load Balancing/NAT Action

Name:

Description:

NAT Type: Virtual IP

Load Balancing: Round Robin

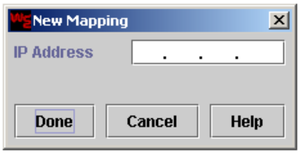
Mappings

5 Type a name and brief description for the dynamic NAT action in the appropriate fields. The **Description** field is optional.

6 Select **Dynamic NAT** from the **NAT Type** drop list.

7 Click **New**.

The New Mapping dialog box appears.



8 Type the publicly routable IP address in the **IP Address** field.

9 Click **Done** to close the **New Mapping** dialog box and return to the **New Load Balancing/NAT Action** dialog box.

10 Click **Done** to close the **New Load Balancing/NAT Action** dialog box.

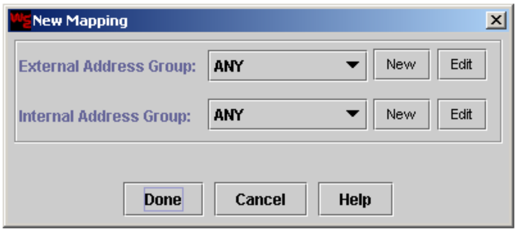
Follow these steps to configure a Static NAT action:

1 Click **New** from the right of the **NAT/Load Balancing** drop list.
The New Load Balancing/NAT Action dialog box appears.

2 Type a name and brief description for the dynamic NAT action in the appropriate fields. The **Description** field is optional.

3 Select **Static NAT** from the **NAT Type** drop list.

4 Click **New**.
The New Mapping dialog box appears.



5 Select an address group from the **External Address Group** and **Internal Address Group** drop lists.

6 If you have not yet created an address group for the external or internal address, click **New**.
For information on creating an address group, see "Defining an address group" on page 126.

7 Click **Done** to close the **New Mapping** dialog box and return to the **New Load Balancing/NAT** dialog box.
The new mapping entry is displayed.

8 Click **Done**.

Defining a Load-Balancing Action

Follow these steps to define a load-balancing action:

1 Click **New** from the right of the **NAT/Load Balancing** drop list.
The New Load Balancing/NAT Action dialog box appears.

2 Type a name and brief description for the load balancing action in the appropriate fields. The **Description** field is optional.

3 Select **Virtual IP** from the **NAT Type** drop list.

4 Select on of the following options from the **Load Balancing Algorithm** drop list:

Round Robin
Each server is treated with equal priority.

Weighted Round Robin
Each server is given priority based on its ability to deliver specific applications.

Random
Traffic is randomly distributed to a series of servers.

Weighted Random
Algorithm weights are assigned to servers based on server capacity limitations.

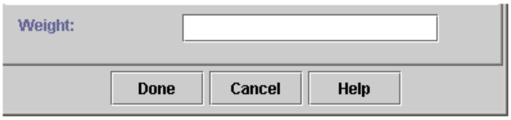
Least Connection
When new traffic is sent to the servers, an algorithm determines which server has the least number of connections.

Weighted Least Connection
When new traffic is sent to the servers, an algorithm determines the least number of connection and weights that can be assigned.

If you chose **Weighted Round Robin**, **Weighted Random**, or **Weighted Least Connection** from the **Load Balancing** drop list, you can assign specific weights to particular IP addresses or address groups.

Follow these steps to assign weights:

1 Click **New**.
The New Mapping dialog box appears and the Weight field is active.



2 Enable one of these options and follow these instructions:

Address Group
Select an option from the drop list.

IP Address
Type the IP address of a server in this field.

3 Type a port number in the **Port** field.

4 Type the number that represents the percentage of load you want to direct to this server in the **Weight** field.

The percentages should be related to the total number of servers and their individual capacities.

5 Click **Done**.

6 Repeat this process as needed to distribute traffic loads to other servers.

Up to 16 servers can be included in a single load-balancing policy.

7 When you are finished, click **Done** to close the **New Load Balancing/ NAT Action** dialog box.

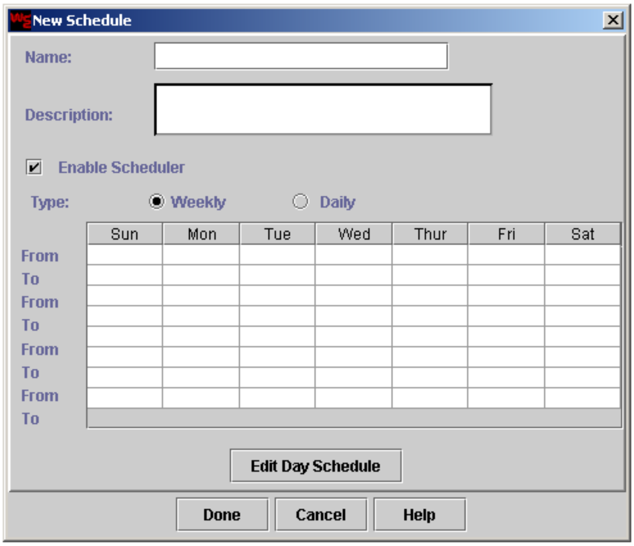
Using Policy Schedules

After a policy is defined and applied, it is in effect immediately, 24 hours a day, seven days a week. However, you can modify a policy such that it is active only during specific times of the day or certain days of the week. For any given day in a week, you can choose up to four periods that a policy will be activated. Outside of that time period, the Firebox Vclass appliance will not apply this policy. Schedules can be formulated within a policy while you create it, or created separately and applied to an existing policy.

Defining a Schedule

Follow these steps to define a schedule:

1 Click **New** from the right of the **Schedule** drop list**.**
The New Schedule dialog box appears.



Name:

Description:

☑ Enable Scheduler

Type: ● Weekly ○ Daily

	Sun	Mon	Tue	Wed	Thur	Fri	Sat
From							
To							
From							
To							
From							
To							
From							
To							

2 Type a name and brief description for the schedule in the appropriate fields. The **Description** field is optional.

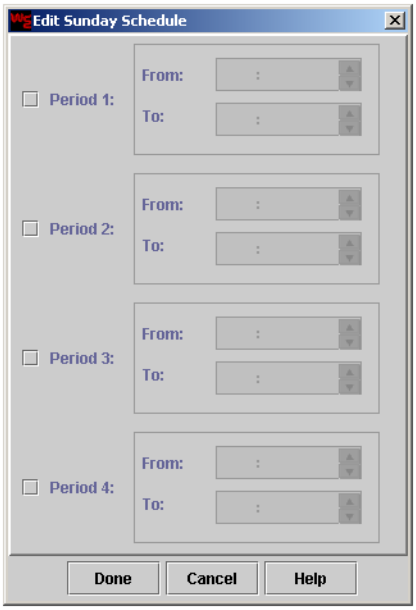
3 If you do not want the policy scheduler to make use of these schedules right away, click to clear the checkbox marked **Enable Scheduler**. You can reopen this schedule and reactivate the Scheduler at a later time.

Follow these steps to create weekly schedules:

1 Select the **Weekly** option.

2 Select the appropriate day you want to schedule.

3 Click **Edit Day Schedule**.
The Edit (Day) Schedule dialog box appears.



4 Click to select the checkbox labeled **Period 1**.

5 Type the values in the **From** and **To** fields, or use the arrow buttons to adjust the values.

NOTE

Remember to type afternoon and evening hours in military time. For example, 1:00 PM must be entered as 13:00.

6 Repeat this process for the remaining periods, as needed.

7 Click **Done**.

8 Repeat this process until a complete week's schedule has been recorded.

9 Click **Done**.

If you want to create a daily schedule that affects every day of the week, follow these steps:

1 Select the **Daily** option.

2 Click **Edit Day Schedule**.
The Edit Day Schedule dialog box appears.

3 Click to select the checkbox labeled **Period 1**.

4 Type the values in the **From** and **To** fields, or use the arrow buttons to adjust the values.

NOTE

Remember to type afternoon and evening hours in military time. For example, 1:00 PM must be entered as 13:00.

5 Repeat this process for the remaining periods, as needed.

6 Click **Done** to close the **Edit Day Schedule** dialog box and return to the **New Schedule** dialog box.

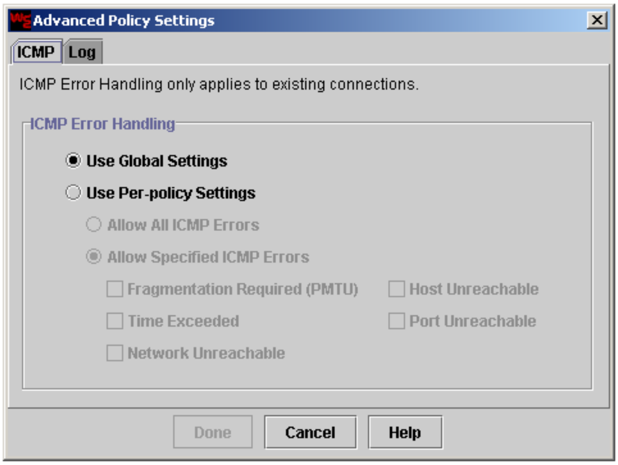
7 Click **Done**.

Using the Advanced Settings

Use the advanced policy settings to create global settings or per policy settings for ICMP error message handling as well as a per policy logging.

Follow these steps to configure the advanced settings:

1 Click **Advanced**.
The Advanced Policy Settings dialog box appears.



ICMP Error Handling only applies to existing connections.

ICMP Error Handling

● Use Global Settings

○ Use Per-policy Settings

○ Allow All ICMP Errors

● Allow Specified ICMP Errors

□ Fragmentation Required (PMTU) □ Host Unreachable

□ Time Exceeded □ Port Unreachable

□ Network Unreachable

2 Click one of the following options:

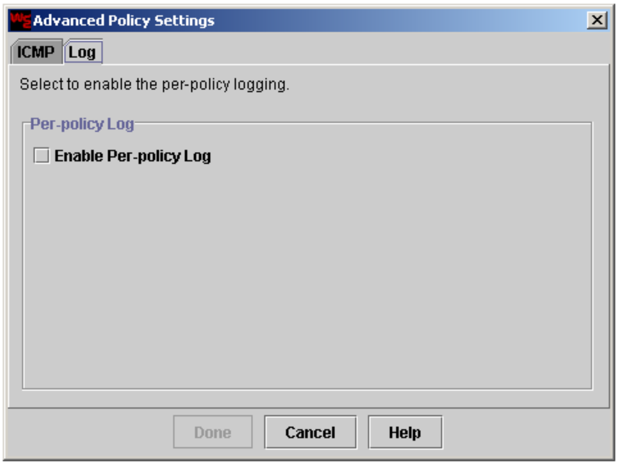
Use Global Settings

Selecting this option enables the ICMP error handling global policy settings configured using the System Configuration button. For more information, see “Advanced Configuration” on page 90.

Use Per-Policy Settings

Selecting this option allows you to define ICMP error handling parameters particularly for this security policy, effectively overriding any global settings you may have configured. Click one of the following options: **Allow All ICMP Errors** or **Allow Specified ICMP Errors**. Selecting the latter allows you to define which ICMP error messages will be allowed through the Firebox Vclass appliance.

3 Click the **Log** tab.



Select to enable the per-policy logging.

□ Enable Per-policy Log

4 To enable the Firebox Vclass appliance to log for this particular security policy, click **Enable Per-policy Log**.

The traffic log setting *must* also be enabled. For more information on configuring logging, see "Log Settings" on page 247.

5 When you have finished, click **Done**.

CHAPTER 8

Security Policy Examples

This chapter includes examples of Vclass Firewall policies, VLAN policies, Quality of Service policies, NAT policies, and Load Balancing policies. You can use these polices as a guide when designing your system security policies.

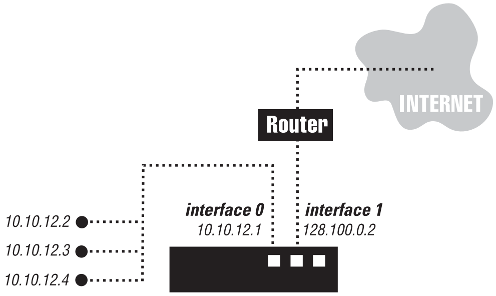
Firewall Policy Examples

The following sections describe different types of networks and how to create firewall policies to meet their security objectives.

Example 1: Allowing Internet access

Westchester Inc. has a small branch office with a limited number of publicly routable IP addresses. This office requires a simple set of firewall policies that allows users to access the Internet while protecting the network from external traffic.

This illustration shows the internal, private network (with private IP addresses assigned to the three computers) as connected to the Private interface of the Firebox Vclass appliance. This interface has its own IP address, and the Public interface (through which all communications with the external networks are routed) has a separate IP address.



You would meet this objective by doing the following:

1 Create two firewall policies with these parameters:

#	Name	Src	Dst	Service	Intrfc	Action	NAT/LB
1	Allow_Private	ANY	ANY	ANY	0	Pass	DYNAMIC_NAT
2	Deny_Public	ANY	ANY	ANY	1	Block	

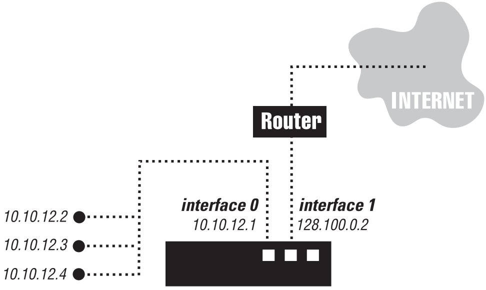
2 Have all the users in the private network reconfigure their computers' default gateway to the IP address of the Private interface on the Firebox Vclass appliance.

Note that Dynamic NAT is applicable only to firewall policies for outgoing traffic.

Example 2: Restricting Internet access

Stillbrook Corporation has a branch office similar to that in example 1: it has a limited number of public IP addresses. However, this company also wants to set the following restrictions on how internal users access the Internet:

- No web surfing (HTTP traffic) during office hours
- Only Web services and email traffic are passed by the Firebox Vclass appliance to the Internet



This example uses the pair of firewall policies created in Example 1. Dynamic NAT provides Internet access for internal users, while another policy protects the private network from external users.

This network also requires two new policies. The first additional policy denies HTTP traffic from the private network using a schedule such that the policy action takes effect only from 9am to 5pm. The second new policy uses the same traffic specifications but passes all HTTP traffic (using dynamic NAT) without any schedule restrictions.

NOTE

If you create a security policy that applies an action according to a schedule, it is a good practice to create an exact duplicate of that policy, with the opposite firewall action without a schedule, that is listed immediately following the scheduled policy. Having such a pair of policies ensures that the same traffic is permitted after the specified schedule expires.

1 Using the **Insert Security Policy** dialog box, set up the following policies, one at a time.

	Name	Src	Dest	Service	In	Firewall	NAT/LB	Schedule
1	Deny_HTTP	ANY	ANY	HTTP	0	Block	DNAT	9to5M-F
2	Allow_HTTP	ANY	ANY	HTTP	0	Pass	DNAT	
3	Allow_MAIL	ANY	ANY	POP3	0	Pass	DNAT	
4	Deny_Private	ANY	ANY	ANY	0	Block		
5	Deny_Public	ANY	ANY	ANY	1	Block		

2 Create a schedule with these parameters:

NAME
9 to 5, Monday - Friday

DESCRIPTION
Schedule for 9:00am - 5:00pm, Monday - Friday

ENABLE SCHEDULER
Checked

TYPE
Weekly

DAYS/HOURS
Monday - Friday, From 9:00 To 17:00

Example 3: Allowing unlimited access for authorized users

Chambers Enterprises, like the company in the previous example, wants to block Internet access during working hours. However, it wants to make exceptions for certain authorized users.

To achieve this, you would make use of the user-authentication firewall feature and replace the “Deny_HTTP” policy with a scheduled “Allow_User” policy. When this revised policy is in effect (during office hours), only authorized users are allowed to gain external access. Unauthorized users are still blocked.

1 Use the Account Manager to create end-user access accounts for each individual to be allowed Internet access during working hours.

2 Distribute login IDs, passwords, and connection instructions to these users so that they can connect through the firewall.

3 Create an "Allow_User" firewall policy using the parameters shown below.

Name	Src	Dest	Service	In	Firewall	NAT/LB	Schedule
Allow_User	ANY	ANY	HTTP	0	Authenticate	Dynamic NAT	9to5M-F
Allow_HTTP	ANY	ANY	HTTP	0	Pass	Dynamic NAT	
Allow_MAIL	ANY	ANY	POP3	0	Pass	Dynamic NAT	
Deny_Private	ANY	ANY	ANY	0	Block		
Deny_Public	ANY	ANY	ANY	0	Block		

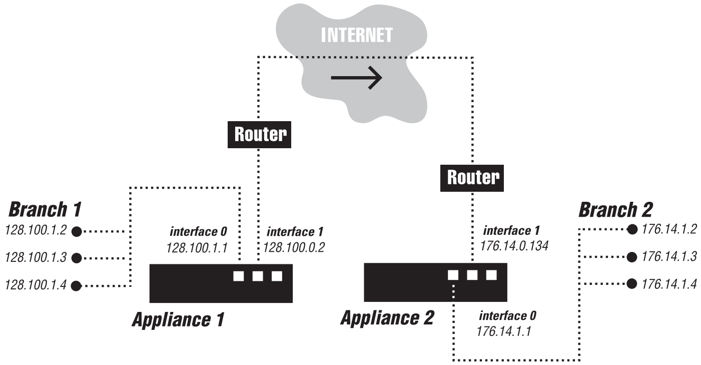
4 Add the "9to5M-F" schedule from Example 2 to this policy so that it takes effect only between 9am and 5pm, Monday through Friday. This permits the "Allow_HTTP" policy to be active outside the specified office hours, at which time all users can surf the Internet.

5 Before this group of authorized users can access the Internet, they must first authenticate their access request so that they can proceed through the firewall. They would do so by entering the following URL in their Web browser: https://126.20.20.1/user.html
In this URL, the "126.20.20.1" entry represents the IP address of interface 0.

Example 4: Allowing communication between branch offices

Appleby Incorporated has two branch offices, each with a separate Firebox Vclass appliance. These branch offices need separate sets of firewall policies to enable all users in the offices to communicate with the other branch office.

To achieve such control over inter-branch traffic, you must create policies on both Firebox Vclass appliances. The following figure illustrates this situation.



A separate policy must be created on each Firebox Vclass appliance so that the users in the private net of the first branch office can access the computers in the private network of the second branch office. The policy on Firebox Vclass appliance 1 specifies the traffic coming in from the private interface, while the policy on Firebox Vclass appliance 2 specifies the traffic coming in from the public interface. Also note that the source, destination, and service have to be exactly the same in both policies.

1 Configure all computers in Branch 1 to use the Private interface of Firebox Vclass appliance 1 as the default gateway.

2 Configure all computers in Branch 2 to use the Private interface of Firebox Vclass appliance 2 as the default gateway.

3 Create two separate address groups to represent the computers in each branch office, using the following entries in the **New Address Group** dialog box:

Address Group 1:

Name: Branch_1, Member type: IP Network, Addresses: 128.100.1.0, Subnet mask: 255.255.255.0

Address Group 2:

Name: Branch_2, Member type: IP Network, Addresses: 176.14.1.0, Subnet mask: 255.255.255.0

4 Create the following policy on Appliance 1:

Name	Src	Dest	Service	In	Firewall
Branch_1to2	Branch_1	Branch_2	ANY	0	Pass

5 Create the following policy on Appliance 2:

Name	Src	Dest	Service	In	Firewall
Branch_1to2	Branch_1	Branch_2	ANY	1	Pass

6 If you want to allow the users in the private network of branch 2 office to access the computers in the private network of branch 1 office, create two more policies on that appliance to permit such traffic. The final list of policies used by the appliances should look like this:

Policies on Appliance 1

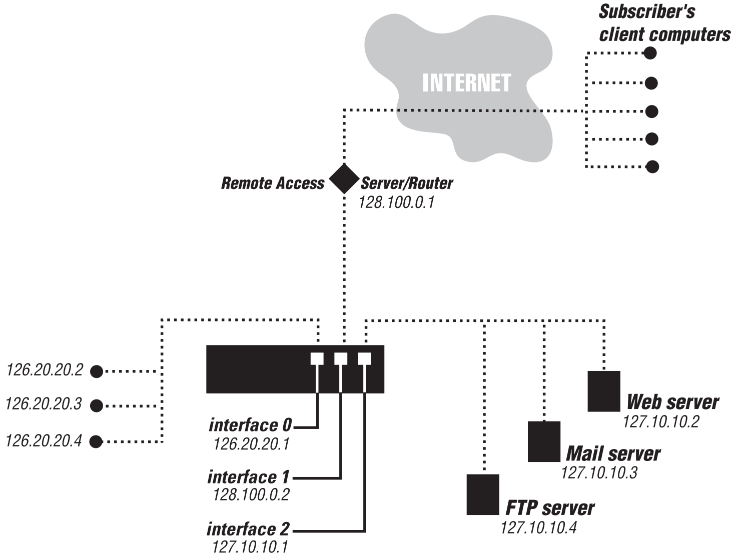
Name	Src	Dest	Service	Incoming	Firewall
Branch_1to2	Branch_1	Branch_2	ANY	0	Pass
Branch_2to1	Branch_2	Branch_1	ANY	1	Pass

Policies on Appliance 2

Name	Src	Dest	Service	Incoming	Firewall
Branch_1to2	Branch_1	Branch_2	ANY	1	Pass
Branch_2to1	Branch_2	Branch_1	ANY	0	Pass

Example 5: Defining policies for an ISP

ConnectYouUp.com is an ISP with a firewall that both protects all internal private network assets while permitting access by subscribers to servers in a DMZ, reading and sending email, surfing the Internet, and taking advantage of FTP services.



In such a network environment, you may want to create a number of complementary policies that permit access by certain users to a limited set of assets (servers), while permitting free external access to all internal users.

1 Open the **System Configuration** dialog box and use the **Route** tab features to add a new route to the appliance. The new route represents the default gateway, which is the remote access server/ router.

Destination	Net Mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	128.100.0.1	1	1

2 Reconfigure all of the computers in the private network to use a default gateway corresponding to interface 0 of the Firebox Vclass appliance. In this example, the gateway is 126.20.20.1.

3 Create three separate policies, permitting access to different servers in the DMZ network.

4 Define an email service for the DMZ interface, enabling subscribers to send email.

5 Create a policy to allow all employees on the Private interface to access the Internet.

When you have finished, the complete set of policies should resemble this list, and be listed in exactly this order in the Policies table:

Name	Src	Dest	Service	In	Firewall
Allow_Public_Webserver	ANY	127.10.10.4*	HTTP	1	Pass
Allow_Subscribers_Email	ANY	127.10.10.3*	Email	1	Pass
Allow_DMZ_SendMail	127.10.10.3*	ANY	Email	2	Pass
Allow_Subscribers_FTP	ANY	127.10.10.2*	FTP	1	Pass
Allow_Outbound	ANY	ANY	ANY	0	Pass

NOTE

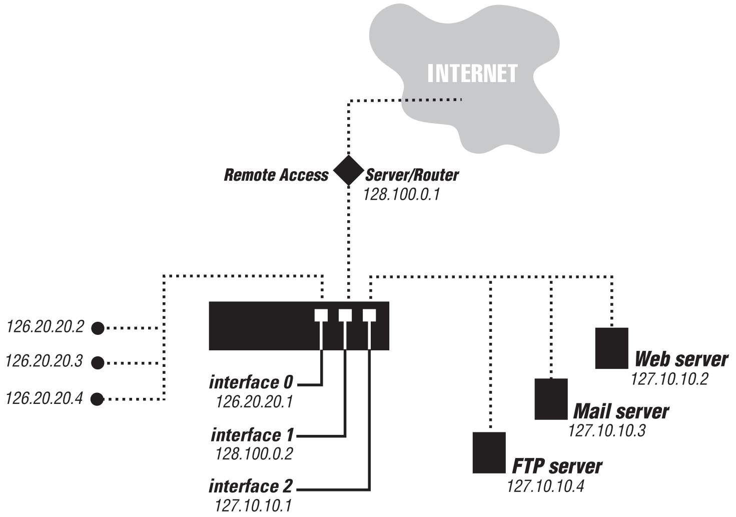
IP addresses are shown for these examples. You must define a separate address group entry for each policy.

Example 6: Controlling access at corporate headquarters

Lubec Corporation wants to augment an existing corporate firewall to provide the following access controls:

- Only authorized internal network users can surf the Internet during working hours. All other users have access only during non-work hours.
- All other types of Internet connections are permitted.

- Everyone from the outside world can send email to the Mail server (accessible through interface 2).



1 Open the **System Configuration** dialog box and use the **Route** tab features to add a new route to the appliance. The new route represents the default gateway, which will be the remote access server.

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	128.100.0.1	1	1

2 All of the computers in the private network must be reconfigured with a default gateway that represents the Private interface of the Firebox Vclass appliance, which in the example is 126.20.20.1.

3 Create a new address group that represents the subnet connected to the private interface of the Firebox Vclass appliance, using these specifications.

Address group 1
Name: HQ

Member type
IP Network Addresses

Address
126.20.20.0

Subnet mask
255.255.255.0

4 Create a schedule called “9to5M-F”, as described in “Example 2: Restricting Internet access” on page 154.

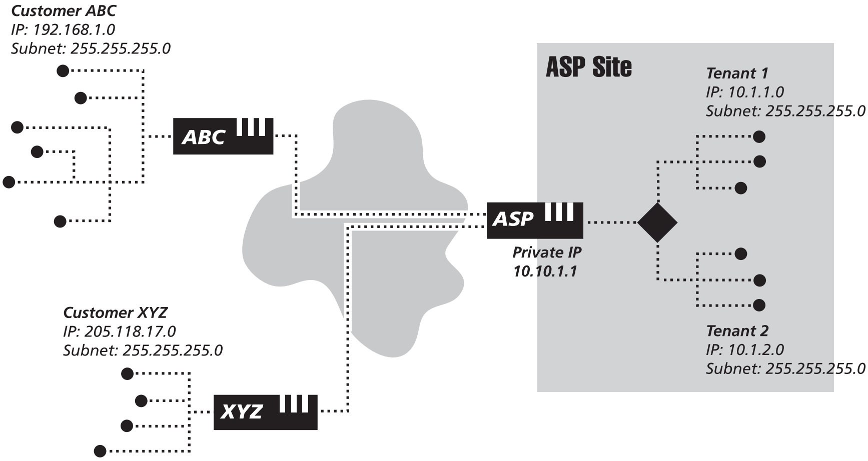
5 Create the necessary end-user accounts for all of the authorized users, as described in “Example 3: Allowing unlimited access for authorized users” on page 156.

6 Create the following security policies in the exact order shown. Note that the user-authenticated firewall policy (the first one to be created) will apply policy actions only to authorized users, while blocking all unauthorized users who are sources of the same type of traffic.

	Name	Src	Dest	Service	In	Firewall	Schedule
1	Allow_User_http	HQ	ANY	HTTP	0	Authenticate	9to5M-F
2	Allow_All_HTTP	HQ	ANY	HTTP	0	Pass	
3	Allow_Private_Any	ANY	ANY	ANY	0	Pass	
4	Allow_Public_Email	ANY	127.10.10.3	Email	1	Pass	
5	Deny_Public	ANY	ANY	ANY	1	Block	

VLAN Policy Examples

The following figure shows how a Firebox Vclass appliance can manage traffic to and from a typical VLAN.



This example consists of an ASP site that hosts two customers' assets:

- Customer ABC's servers are in network 10.1.1.0/255.255.255.0, which has been assigned VLAN ID 3.
- Customer XYZ's servers are in network 10.1.2.0/255.255.255.0, which has been assigned VLAN ID 25.

To make this work, the needed VPN policies are applied in the ASP's security appliance to allow Company ABC and XYZ to access their assets in the ASP through secure VPN tunnels. Because the ASP should not be allowed to access Company ABC and XYZ's private networks, uni-directional VPN policies on the WatchGuard appliances are necessary.

The following address groups and VLAN objects for use by that appliance are required:

Address groups

ABC_Net	IP Address: 192.168.1.0 Subnet Mask: 255.255.255.0
XYZ_Net:	IP Address: 205.118.17.0 Subnet Mask: 255.255.255.0
Tenant_ABC:	IP Address: 10.1.1.0 Subnet Mask: 255.255.255.0
Tenant_XYZ:	IP Address: 10.1.2.0 Subnet Mask: 255.255.255.0

VLAN tenant entries

ABC:	VLAN id = 3 interface 0 (Private) VLAN IP/mask: 10.1.1.1/255.255.255.0
XYZ:	VLAN id = 25 interface 0 (Private) VLAN IP/mask: 10.1.2.1/255.255.255.0

The requisite VPN policies on "ASP" should have the following parameters:

SRC	Dest	Service	In	Tenant	Firewall	IPSec
ABC_Net	Tenant_ABC	ANY	1	ABC	Pass	—> ipsec_ABC
XYZ_Net	Tenant_XYZ	ANY	1	XYZ	Pass	—>ipsec_XYZ

At the Company ABC site, a new policy should be applied to "ABC" with the following parameters:

SRC	Dest	Service	In	Tenant	Firewall	IPSec
ABC_Net	Tenant_ABC	ANY	0		Pass	<— ipsec_ABC

At the Company XYZ site, a new policy should be applied to "XYZ" with the following parameters:

Src	Dest	Service	In	Tenant	Firewall	IPSec
XYZ_Net	Tenant_XYZ	ANY	0		Pass	<— ipsec_XYZ

Using a Firebox Vclass appliance in a VLAN setting

If your SNMP management stations, DNS servers, OSPF routers, RADIUS servers, and mail servers are located in a VLAN-enabled network, you must explicitly define separate policies that allow Firebox Vclass appliances to send traffic to those devices. Otherwise, some Firebox Vclass features, such as SNMP trap notification and DNS lookup, will not work. Here is an example of a policy that allows SNMP traps sent from a Firebox Vclass security appliance to a SNMP management station in VLAN 20.

Src	Dest	Service	In	Tenant	Firewall
PRIVATE_PORT_IP	SNMP_STATION	SNMP trap	Internal	VLAN_20	Pass

Creating policies for user-domain tenants

In addition to VLAN tenant-specific policies, the Vcontroller permits you to set up user domain–specific policies, which enable the appliance to perform traffic management for multi-tenant domains without the attendant VLAN hardware.

The concept behind the definition of a user domain tenant involves identifying the tenant and establishing the means of authenticating that tenant. For example, the Vcontroller administrator first defines a new user domain tenant (as described in this section). At this time, the administrator must link this entry to the relevant RADIUS system to provide authentication services. Next, the administrator can create the policies necessary for this user domain (and the tenants).

When a user domain tenant wants to initiate an Internet or other external network connection through the Firebox Vclass appliance, he or she would first log into the appliance using the user name, password, and domain name previously defined in the tenant record. After this is verified by the RADIUS system, the Firebox appliance associates the user (IP address) to the relevant domain. Any traffic from the user will then be covered by policies that incorporate that domain.

An example of a user-domain policy in use

As noted previously, the key element in user-domain tenant policies is *user authentication*. This is how traffic pertaining to a specific tenant is identified. For example:

- The Vcontroller administrator creates a user-domain tenant record for "Engineering" domain users that uses a RADIUS server for user authentication.
- Policies are created to manage traffic for an external network, originating from "Engineering."
- When one of the tenant users wants to make an external connection, he or she opens a Web browser and logs into the Firebox appliance. The user's IP address is also noted by the appliance.
- After the user provides a user name, password, and domain name (specified in the Tenant entry as referenced by the policy), his or her name and password are validated by the RADIUS system.
- The user is granted access to the external network.
- The appliance now classifies packets from the user's computer as traffic from the "Engineering" domain tenant.
- Finally, after a set idle time expires, the connection is broken, and that user will have to log in and re-authenticate before being granted access to the external network again.

One of the advantages of creating and applying user-domain tenants to policies is that there is no strict relationship between a tenant and the originating computer's IP address. The computer used by a tenant user is noted dynamically by the appliance during the authentication process; the user name, password, and domain are the key, and the IP address simply becomes a temporary location for the duration of the connection.

QoS Policy Examples

When using QoS actions within your policies to prioritize your network traffic, remember that any traffic streams not included in explicit QoS actions will be affected by a default QoS action with WFQ set to 5. The following example shows how this works in conjunction with other QoS policies.

Example 1:

Policy 1: QoS action A with WFQ weight = 5

Policy 2: No QoS

Policy 3: No QoS

Policy 4: QoS action B with WFQ weight = 10

Policy 5: No QoS

In this case, the ratio between all three QoS actions is 5 (default), 5 (QoS A), and 10 (QoS B). When the network bandwidth is fully utilized, policy 1 traffic will use 25% of the bandwidth, policy 4 will use 50%, and all other traffic will share the remaining 25%.

Example 2:

Policy 1: QoS action A with WFQ weight = 15

Policy 2: No QoS

Policy 3: No QoS

Policy 4: QoS action B with WFQ weight = 5

Policy 5: No QoS

Policy 6: QoS action B with WFQ weight = 5

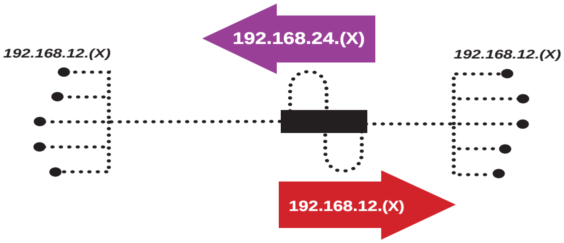
In this case, the ratio between all three QoS actions is 5 (default), 15 (QoS A), and 5 (QoS B) which is a 1:3:1 ratio. Therefore, when the network capacity is fully utilized, policy 1 traffic will use 60% of the total bandwidth (3/5), policy 4 and policy 6 traffic will share 20% (1/5) of the bandwidth, and all other traffic will share the remaining 20% (1/5) of bandwidth.

Static NAT Policy Examples

The following sections describe different examples of static NAT applications.

Example 1: Translating IP addresses into aliases

If one region of your network is protected from unauthorized internal use connections, it may rely on a pool of internal-use IP addresses that are also used in other network regions. You can set up a static NAT policy that translates the existing IP addresses into aliases, for use in establishing connections with other regions of the network without fear of IP address conflicts.



The policies would incorporate these entries:.

	Name	Source	Dest	Service	In	Static NAT action
1	Inbound static NAT	ANY	Alias	ANY	1	static NAT_1
2	Outbound static NAT	Internal_Net	ANY	ANY	0	static NAT_1

The two address groups would include these entries:

Internal_net
192.168.12.0/24

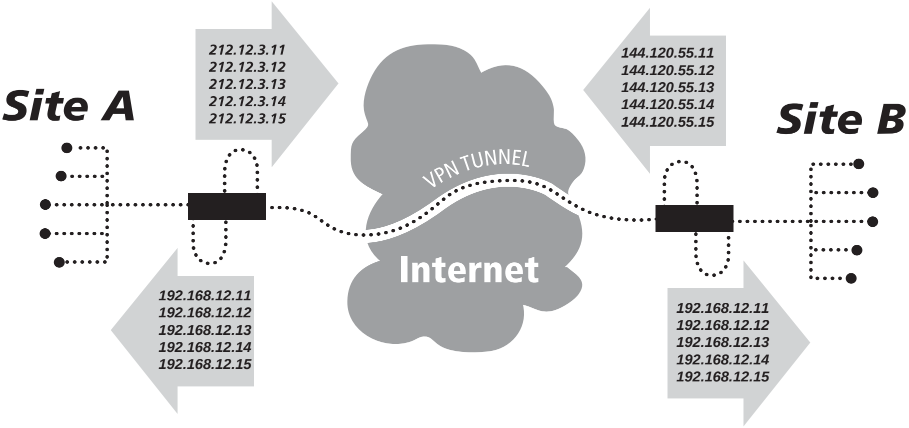
Alias
192.168.24.0/24

The static NAT action would reflect these entries:

static NAT_1
Internal = Internal_net
External = Alias

Example 2: Preventing conflicts between IP addresses

If your extended network relies on VPN connections between gateway appliances at remote sites, you can set up address translation to prevent conflicts between the common pools used in the internal networks behind each appliance.



These address groups must first be entered in Vcontroller in the respective locations:

For Site A	Net_A: 192.168.12.0/24 Alias_A: 212.12.3.0/24 Net_B: 144.120.55.0/24
For Site B:	Net_B: 192.168.12.0/24 Alias_B: 144.120.55.0/24 Net_A: 212.12.3.0/24

The following static NAT actions must be entered in Vcontroller in the respective locations:

For Site A	static NAT_A Internal: Net_A External: Alias_A
For Site B	static NAT_B Internal: Net_B External: Alias_B

The policies in the Site A security appliance would include these settings:

	Name	Src	Dest	Service	In	Static NAT action	
1	SITE_A-B	Net_A	Net_B	ANY	0 (pvt)	static NAT_A	IPSec_A-B (<->)

The policies in the Site B security appliance would include these settings:

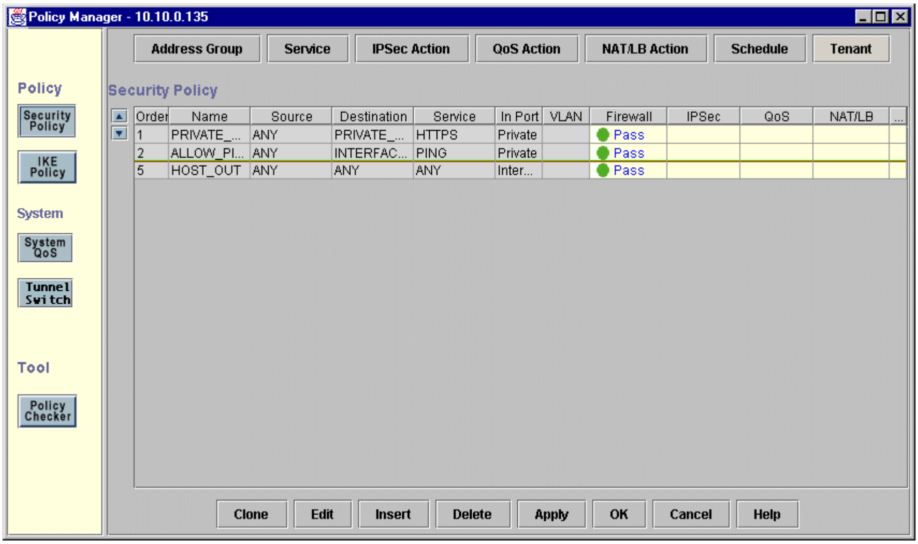
	Name	Src	Dest	Service	In	static NAT action	
1	SITE_B-A	Net_B	Net_A	ANY	0 (pvt)	static NAT_b	IPSec_A-B (<->)

Load Balancing Policy Examples

Configuring Load Balancing for a Web Server

1 After starting the Vcontroller application, click **Security Policy** in the Policy column.

The Policy Manager window appears.



Security Policy

Order	Name	Source	Destination	Service	In Port	VLAN	Firewall	IPSec	QoS	NAT/LB	...
1	PRIVATE_...	ANY	PRIVATE_...	HTTPS	Private		● Pass				
2	ALLOW_PI...	ANY	INTERFAC...	PING	Private		● Pass				
5	HOST_OUT	ANY	ANY	ANY	Inter...		● Pass				

2 Click any existing policy entries (or click the last row) in the **Security Policies** list.

Your new policy appears in the row you selected and moves the existing policy down a row.

NOTE

If your Firebox Vclass appliance is already using a "block all external traffic" firewall policy, this new load-balancing policy must be listed above the firewall policy.

3 Click the **Insert** button at the bottom of the window.

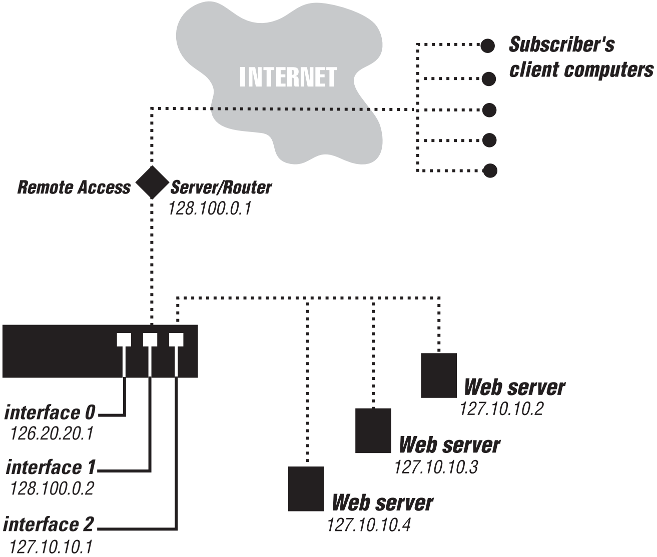
The Insert Security Policy dialog box appears.

4 Type a name and brief description for the policy in the appropriate fields. The **Description** field is optional.

Configuring Load Balancing for an E-commerce Site

The following example shows how a Firebox Vclass appliance can function as a load balancing accessory to evenly distribute data requests to a series of Web servers. This scenario can be adapted to full effect in e-commerce sites that use a large number of servers to manage the growing number of consumers.

An e-commerce site may get several hundred thousand hits a day. A Firebox Vclass appliance can be strategically placed in the network to function as both a firewall that protects internal network assets and a load balancer for the Web servers.



In this scenario, any number of external client users will be trying to connect to a Web site with a URL that points solely to a single, publicly routable IP address, 128.100.0.2. This address cannot be shared by all the existing Web servers, each of which has its own internal IP address. The challenge is to evenly distribute each new data request to a different server, although the requests originally expect 128.100.0.2 to answer.

1 Open the **System Configuration** dialog box and use the **Route** tab to either add a default gateway or change the existing default gateway to 128.100.0.1.

2 Open the **Insert Security Policy** dialog box and make the following entries.

	Name	Source	Destination	Service	Incoming	Firewall
1	Allow_HTTP	ANY	127.10.10.0	HTTP	1	Pass

Consider what would happen if the above firewall policy is the only one implemented. Clients attempting to access Web servers in the DMZ network will endure long wait times. The existing Web servers cannot share the total load of HTTP requests. If one of the Web servers is overloaded with requests, the other two Web servers will not pick up the excess requests automatically.

A load balancing policy fixes these problems. Because all clients use the publicly routable IP address (128.100.0.2), the Firebox Vclass appliance automatically receives all such requests and distributes them to the Web servers in the DMZ net, regardless of what IP addresses each Web server is assigned.

In this example, the site's publicly routable IP address will be assigned to the appliance's Public interface. The resulting load balancing policy will distribute HTTP requests to each of the Web servers in turn:

1 Reopen the firewall policy.

2 Change the **Destination** to "128.100.0.2".

3 Click the **New** button to the right of the **NAT/LB Action** drop list.

4 When the **New NAT Action** dialog box appears, enter a name for the new action, such as `Web-load`.

5 From the **NAT Type** drop list, select **Virtual IP**.

6 From the **Load Balancing Algorithm**, select **Weighted Least Connection**.

The Firebox Vclass appliance will route incoming HTTP traffic to the Web server that has the least number of active requests among the three servers.

7 Click **New** to the right of the **Servers** list.

8 When the **New Server** dialog box appears, select **IP Address** and type "127.10.10.2" in the accompanying text field.

9 In the **Port** field, type "80", unless there is another port number for this server.

10 In the **Weight** field, type "1".

Weight establishes the load/capacity of all the Web servers in proportion to each other. The specific number can be determined using the following formula, as shown in these two examples:

Load/Capacity
First Web server1
Second Web server2 (twice as much as the first Web server)
Third Web server3 (three times as much as the first Web server)
The weight distribution for these Web servers would be 1:2:3.

Load/Capacity
First Web server1
Second Web server1 (same as the first Web server)
Third Web server2 (twice as much as the first Web server)
The weight distribution for these Web servers would be 1:1:2.

11 Click **Done** to save the new server entry.

12 Repeat the **New Server** dialog box process two more times and enter the separate IP addresses of the other two Web servers. Use the Weight numbers "2" and "3" in each case.

13 When you have saved all three server entries, click **Done** to save this NAT/LB action.

14 Save your new policy and then apply it in the Policy Manager window.

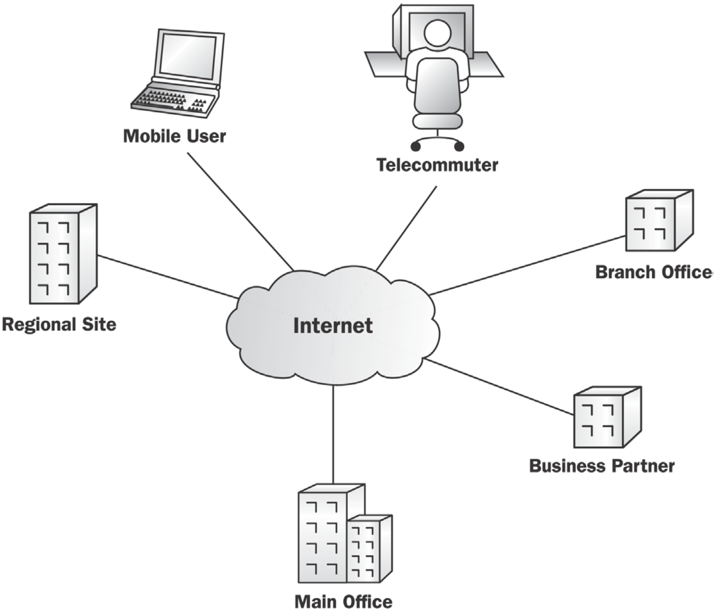
The final load balancing policy will have these settings:

	Name	Src	Dest	Service	In	Firewall	NAT/LB
1	Allow_HTTP	ANY	128.100.0.2	HTTP	1	Pass	Web-Load

CHAPTER 9

Using Virtual Private Networks (VPN)

The Internet is a technical and social development that puts a multitude of information at your fingertips. On this worldwide system of networks, a user at one computer can get information from any other computer. The benefits of using the Internet to exchange information and conduct business are enormous. Unfortunately, so are the risks. Because data packets traveling the Internet are transported in plain text, potentially anyone can read them and place the security of your network in jeopardy.



Virtual private networking technology counters this threat by using the Internet's vast capabilities while reducing its security risk. A virtual private network (VPN) allows communication to flow across the Internet between two networks or between a host and a network in a secure manner. The networks and hosts at the endpoints of a VPN are typically corporate headquarters, branch offices, remote users, telecommuters, and traveling employees. User authentication verifies the identity of both the sender and the receiver. Data sent by way of the Internet is encrypted such that only the sender and the receiver of the message can see it in a clearly readable state.

About VPN Policies

To establish VPN connections between your present site and other remote sites, you must create and apply VPN policies in security appliances on each end. These policies specify the required levels of authentication and encryption to protect the data. In addition, you can also create VPN policies that permit secure communications between a site and authorized clients.

VPN policies and IPSec actions

A VPN security policy always includes an *IPSec action*, regardless of whether you are creating a manual key or automatic key policy. The IPSec action determines what type of authentication and encryption is used to protect traffic governed by this policy. VPN policies can incorporate different kinds of keys (manual or automatic) and different types of encryption and authentication algorithms to be applied to the data stream. If a VPN policy has no IPSec action, the data will be sent as clear text.

Three major qualifications are established in an IPSec action:

Mode

Tunnel mode is used when Firebox Vclass appliances act as security gateways on both ends or when a remote Firebox Vclass VPN client connects to a Firebox Vclass security appliance. Data packets are encrypted and tunnelled from one appliance to the other, where decryption takes place and the data is forwarded to its final destination. The IP address of each tunnel peer must be specified.

Transport mode is usually applied in end-to-end secured communications.

Key Management

This specifies whether the key is automatically or manually created. Automatic key management is done in accordance with IKE, an IETF standard protocol. Using IKE, encryption keys are automatically negotiated and selected by two connected security appliances. This provides the easiest, most efficient key management.

Encryption/authentication

Two principal types of security protocols exist to protect data packets in Internet communications. AH (Authentication Header) protocol is applied to IP packets for authentication, while ESP (Encapsulating Security Payload) can be applied to IP packets for both encryption and authentication.

About Authentication and Encryption

The Firebox Vclass security appliance supports the following algorithms:

Authentication Header (AH)
MD5, SHA

Encapsulating Security Payload (ESP)
DES, 3DES

When an automatic key is configured in an IPSec action, authentication and encryption must be selected. These keys are created by the administrator. Using a manual key provides more flexibility regarding which authentication methods and encryption algorithms are used.

This flexibility is expressed in the form of proposals incorporated into the IPSec action. For example, one proposal may use ESP with 3DES for encryption and SHA for authentication. A second proposal uses ESP with DES for encryption and AH with MD5 for authentication. When a Firebox Vclass appliance negotiates with another appliance to select an automatic key, the initiating appliance sends a list of proposals to the other, starting a negotiation process at the end of which a protocol and algorithm are chosen and used.

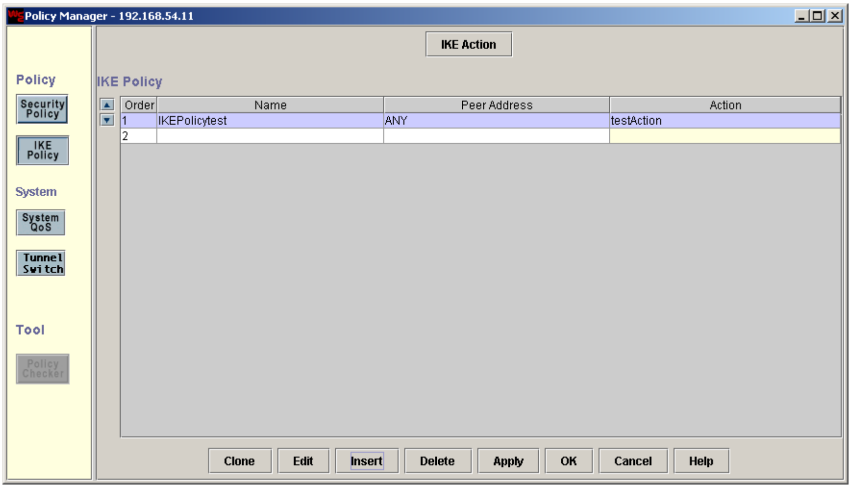
NOTE

You must activate your LiveSecurity Service to enable 3DES encryption.
To activate your LiveSecurity Service, go to:
http:\\www.watchguard.com\activate
For more information on LiveSecurity Service, see "Service and Support" on page 7.

Defining an IKE Policy

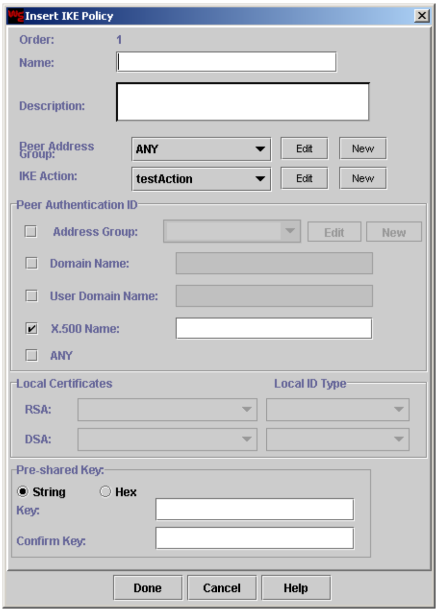
Follow these steps to define an IKE policy:

1 From the main Vcontroller page, click **IKE Policy**.
The IKE Policy dialog box appears.



Order	Name	Peer Address	Action
1	IKEPolicytest	ANY	testAction
2			

2 Select an entry point among the list of policies and then click **Insert**.
The Insert IKE Policy dialog box appears.



Order: 1
Name:
Description:
Peer Address Group: ANY
IKE Action: testAction

□ Address Group:
□ Domain Name:
□ User Domain Name:
☑ X.500 Name:
□ ANY

RSA:
DSA:

● String ○ Hex
Key:
Confirm Key:

3 Type a name and brief description for the IKE policy in the appropriate fields. The **Description** field is optional.

4 Select a preconfigured address group from the **Peer Address Group** drop list or click **New** to create a new address group. For information on creating an address group, see "Defining an address group" on page 126.

5 Select a preconfigured **IKE Action** from the drop list or click **New** to create a new IKE action. For information on creating an IKE action, see "Defining an IKE action" on page 183.

6 From the **Peer Authentication ID** field, select one of the following options:

Address Group
Select the address group of the remote gateway from the drop list, or click **New** to create a new address group. For information on creating an address group, see "Defining an address group" on page 126.

Domain Name
Type the domain name of the remote gateway.

User Domain Name
Type the user domain name of the remote gateway.

X.500 Name
Type the X.500 certificate name used by the remote gateway.

Any
This allows any traffic from the remote gateway to initiate the IKE policy. No ID will be verified.

7 If you previously selected an IKE action that incorporates RSA or DSA as the authentication type, the **Local Certificates** options become active and the RSA or DSA drop lists become active. From the drop list, select the appropriate certificate. Next, select the **Local ID Type** from the drop list. This should be one that the peer system can validate with a copy of your certificate sent to the peer system as well as settings in their own policy.

8 If you previously selected an IKE action that incorporates the pre-shared key authentication type, the **Pre-Shared Key** options become active.

NOTE

This key will be shared among all participating peer IKE systems. If a remote peer does not use the same key, or if a different authentication is used, negotiations will fail.

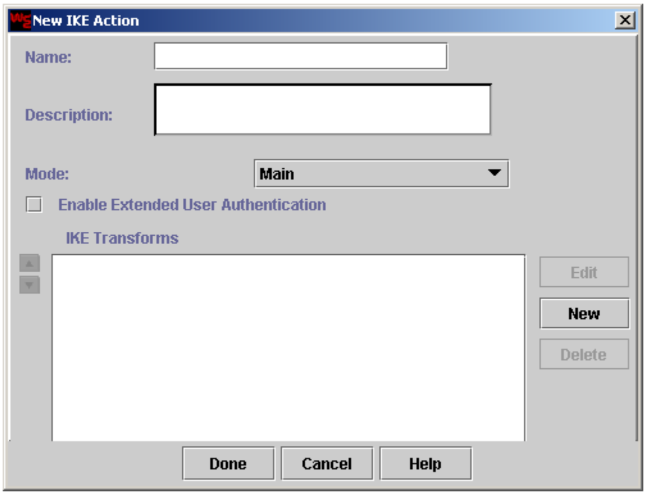
9 Click either **String** or **Hex**, and then type and confirm the key in the fields.
The key can consist of any combination of letters and numbers, but it cannot contain blank spaces.

10 Click **Done** to return to the IKE Policy page.

Defining an IKE action

Your choice of IKE action defines how IKE peers authenticate each other and which encryption is used to protect the negotiation process.

1 From the right of the **IKE Action** drop list, click **New**.
The New IKE Action dialog box appears.



2 Type a name and brief description for the IKE action in the appropriate fields. The **Description** field is optional.

3 From the **Mode** drop list, select one of these options:

Main

A slower mode that provides greater security. This is the recommended mode.

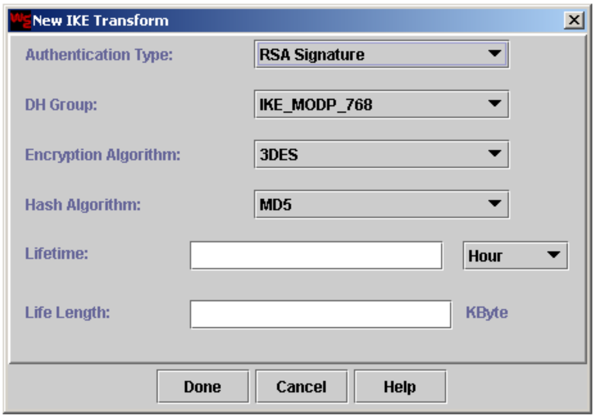
Aggressive

A faster, less secure mode. If you choose this mode, you can include only one IKE transform.

4 If you selected the **Main** mode from the drop list, you can enable **Extended User Authentication** by clicking the appropriate checkbox.

5 Select an IKE transform from the list or click **New** to create a new IKE transform.

The New IKE Transform dialog box appears.



New IKE Transform

Authentication Type: RSA Signature

DH Group: IKE_MODP_768

Encryption Algorithm: 3DES

Hash Algorithm: MD5

Lifetime: Hour

Life Length: KByte

6 Select an **Authentication Type** from the drop list

7 Select a **DH Group** from the drop list.

DH (Diffie-Helman) groups enable two peer systems to publicly exchange and agree on a shared secret key. The numbers available on the drop list (768 and 1024) are the number of bits used for exponentiation to generate private and public keys. The larger the number, the greater the protection.

8 Select an **Encryption Algorithm** from the drop list.

9 Select a **Hash Algorithm** from the drop list.

10 Type the number of hours or minutes that the transform will remain active in the **Lifetimes** field.

11 Select **Hours** or **Minutes** from the **Lifetime** drop list.

12 Type the maximum size in kilobytes in the **Life Length** field. This field is optional.

13 Click **Done**.

The transform is added to the IKE transforms list.

14 Repeat this process to add any other transforms.

Aggressive mode permits only a single transform.

15 When all the required transforms are listed, you can shuffle the order, if necessary, by selecting a transform and clicking the Up or Down arrows to the left of the list.

The order in which transforms are listed establishes the preference order of all listed transforms during phase one negotiations.

16 Click **Done**.

Defining a VPN Security Policy

This section provides information on defining a VPN security policy that creates a VPN connection between two Firebox Vclass appliances.

NOTE

If you want to permit connections that exchange traffic in both directions, you must create a single bidirectional VPN policy. You cannot create two mirroring unidirectional VPN policies, one that permits inbound traffic and one for outbound traffic.

1 From the main Vcontroller page, click **Security Policy**.

The Security Policy dialog box appears.

2 Select an entry point among the list of policies and then click **Insert**.

The Insert Security Policy dialog box appears.

3 Type a name and brief description for the security policy in the appropriate fields. The **Description** field is optional.

4 Select a preconfigured address group from the **Source** drop list corresponding to the remote appliance or click **New** to create a new address group. For information on creating an address group, see “Defining an address group” on page 126.

5 Select a preconfigured address group from the **Destination** drop list corresponding to the local appliance or click **New** to create a new

address group. For information on creating an address group, see "Defining an address group" on page 126.

6 Select a preconfigured **Service** from the drop list or click **New** to create a new service. For information on creating a service, see "Defining a service" on page 128.

7 Select an **Incoming Interface** from the drop list.

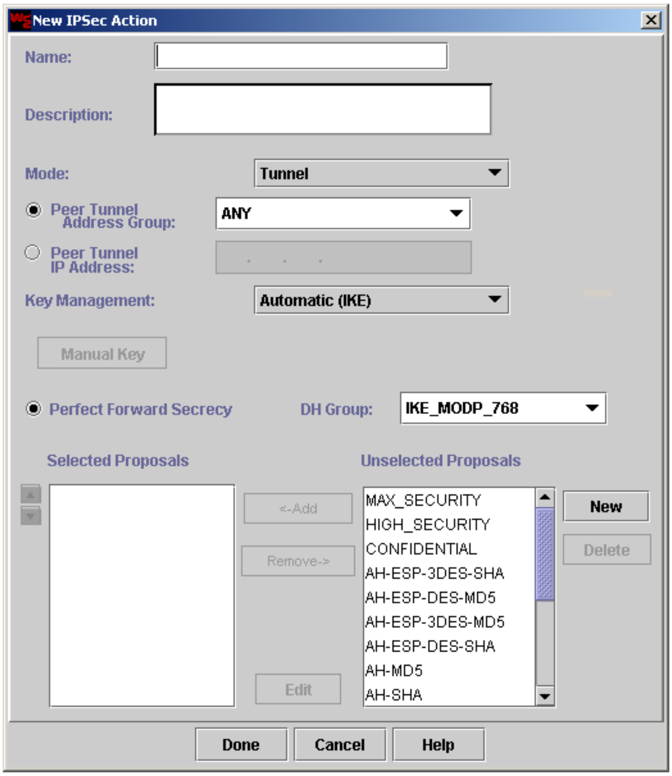
NOTE

If this a bidirectional policy, make sure that the incoming interface selection is 0 or 2, and not 1.

Defining an IPSec action

Follow these steps to define an IPSec action:

1 At the right of the **IPSec** drop list, click **New**.
The New IPSec Action dialog box appears.



New IPSec Action

Name:

Description:

Mode: Tunnel

● Peer Tunnel Address Group: ANY

○ Peer Tunnel IP Address: . . .

Key Management: Automatic (IKE)

● Perfect Forward Secrecy DH Group: IKE_MODP_768

Selected Proposals

Unselected Proposals

MAX_SECURITY
HIGH_SECURITY
CONFIDENTIAL
AH-ESP-3DES-SHA
AH-ESP-DES-MD5
AH-ESP-3DES-MD5
AH-ESP-DES-SHA
AH-MD5
AH-SHA

2 Type a name and brief description for the IPSec action in the appropriate fields. The **Description** field is optional.

3 Select an option from the **Mode** drop list:

Tunnel

This policy prompts the Firebox Vclass appliance to hide any information about the original sender of data, representing the Firebox Vclass appliance as the original sender. This option is preferred for site-to-site connections, in which the traffic goes through the Firebox Vclass appliance.

Transport

No additional identity masking is applied. This option is generally used in secured communication directed to this Firebox Vclass appliance, such as SNMP traffic.

4 If you selected **Tunnel**, you have two options:

   - Click the **Peer Tunnel Address Group** option and then select the address group that represents the peer IP address of the tunnel from the drop list.
   - Click the **Peer Tunnel IP Address** option and then type the peer IP address.

5 From the **Key Management** drop list, select one of the following options:

Automatic (IKE)

This key management process regularly replaces existing keys with randomly generated keys that are created by the Firebox Vclass system. For information on creating an automatic key, see “Defining an automatic key” on page 189.

Manual

Manual key mode requires that the administrator of each security appliance manually enter the text of a key on each system that exactly matches the other system’s key. The drawbacks to manual keys are potential errors in entry, the need to manually replace keys on a regular basis, and the vulnerability of a fixed key to hacking attempts.

For information on creating a manual key, see “Defining a manual key” on page 193.

6 If you want to permit connections initiated in both directions, click the checkbox labeled **Gateway to Gateway VPN**.

NOTE

If this a bidirectional policy, make sure that the incoming interface selection is 0 or 2, and not 1.

7 For information on configuring the remaining options of the policy (QoS action, TOS Marking, NAT/Load Balancing, Scheduling, and the Advanced Settings) see those sections in chapter 7, “About Security Policies” on page 113.

8 Click **Done**.

9 When you have finished configuring VPN policies, click **Apply** to save the settings to the Firebox Vclass appliance.

Defining an automatic key

Automatic key mode requires use of the *Internet Key Exchange* protocol (IKE) to generate new keys when needed. Keys and encryption and authentication algorithms are first negotiated, and then chosen and used by the two participating security appliances.

Follow these steps to define an automatic key:

1 Select Automatic (IKE) from the **Key Management** drop list.

2 If you choose, enable **Perfect Forward Secrecy**.

If you select this checkbox, this policy uses new key material every time it generates a replacement key. If you do not select this checkbox, key replacement uses the source key material that generated previous keys.

3 If you selected Perfect Forward Secrecy, select a **DH Group** from the drop list.

DH (Diffie-Helman) groups enable two peer systems to publicly exchange and agree on a shared secret key. The numbers available on the drop list (768 and 1024) are the number of bits used for exponentiation to generate private and public keys. The larger the number, the greater the protection.

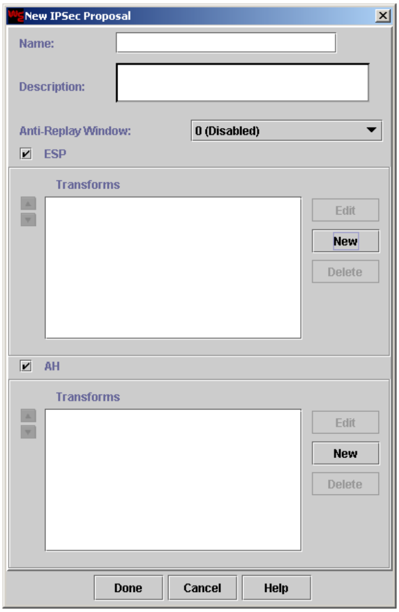
4 Review the default encryption options listed in the **Unselected Proposals** list, select any options that your new IPSec action requires, and click **Add**.

The proposal is displayed in the Selected Proposals field.

If none of the unselected proposals meets the requirements of this automatic key IPSec action, you can create your own proposals.

1 Click **New**.

The New IPSec Proposal dialog box appears.



Name:

Description:

Anti-Replay Window: 0 (Disabled)

☑ ESP

☑ AH

2 Type a name and brief description for the IPSec proposal in the appropriate fields. The **Description** field is optional.

3 Select an option from the **Anti-Replay** window.

These options can protect your system from replay attacks.

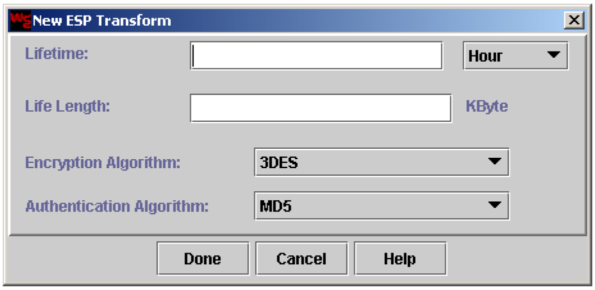
You can now add an ESP transform, AH transform, or both to this proposal. A *transform* defines the encryption and authentication algorithms used by the Firebox Vclass appliance along with setting the lifetime of any given key. ESP transforms are recommended because they incorporate both encryption and authentication of your data.

Follow these steps to define an ESP transform:

1 Select the checkbox labeled **ESP**.

2 Click **New** from the ESP field.

The New ESP Transform dialog box appears



Lifetime: Hour

Life Length: KByte

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

3 Type the number of hours or minutes a key will be in effect in the **Lifetime** field.

If you type zero, this key will have an unlimited lifetime.

4 Select either **Hours** or **Minutes** from the **Lifetime** drop list.

5 Type the maximum number of kilobytes of traffic that would be encrypted by this key before it expires in the **Life Length** field.

If you type zero, there is no maximum limit to the amount of traffic encrypted by this key.

NOTE

Either Lifetime or Life Length must be a non-zero entry.

6 Select an **Encryption Algorithm** from the drop list.

7 Select an **Authentication Algorithm** from the drop list.

8 Click **Done**.

NOTE

You cannot choose **None** for both encryption and authentication when creating an ESP transform.

9 Repeat this process to create additional ESP transforms.

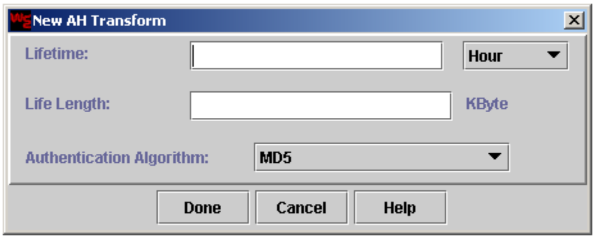
10 You can use the arrow keys to the left of the transforms list to reorganize your newly listed transforms into the proper order of application. Click a transform to move and click the up or down arrow until it appears in the proper place.

The order of transforms represents the preference of the encryption/authentication algorithm and lifetime of keys in this security protocol. Only one of the transforms is chosen when negotiation is complete. If none of the transforms are matched by the peer appliance, the proposal is rejected.

11 When you are finished, click **Done**.

Follow these steps to define an AH transform:

1 Select the checkbox marked **AH**. Click **New** to open the **New AH Transform** dialog box.



New AH Transform

Lifetime: Hour

Life Length: KByte

Authentication Algorithm: MD5

2 Type the number of hours or minutes a key will be in effect in the **Lifetime** field.

If you type zero, this key will have an unlimited lifetime.

3 Select either **Hours** or **Minutes** from the **Lifetime** drop list.

4 Type the maximum number of kilobytes of traffic that would be encrypted by this key before it expires in the **Life Length** field.

If you type zero, there is no maximum limit to the amount of traffic encrypted by this key.

NOTE

Either Lifetime or Life Length must be a non-zero entry.

5 Select an **Encryption Algorithm** from the drop list.

6 Select an **Authentication Algorithm** from the drop list.

7 Click **Done**.

8 Repeat this process to create additional AH transforms.

9 You can use the arrow keys to the left of the transforms list to reorganize your newly listed transforms into the proper order of application. Click a transform to move and click the up or down arrow until it appears in the proper place.

The order of transforms represents the preference of the encryption/authentication algorithm and lifetime of keys in this security protocol. Only one of the transforms is chosen when negotiation is complete. If none of the transforms are matched by the peer appliance, the proposal is rejected.

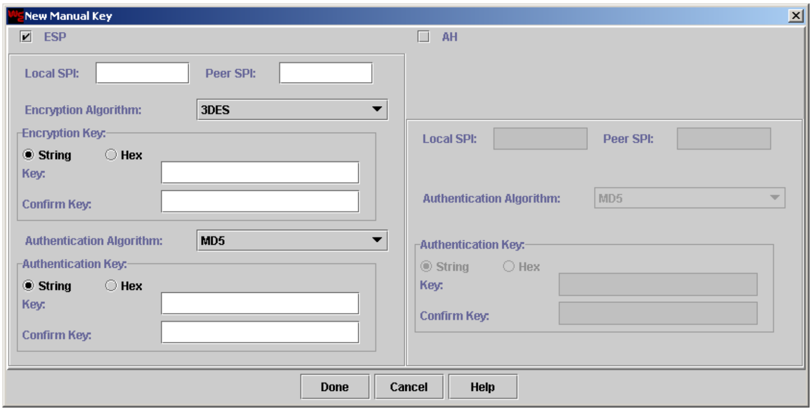
10 When you are finished, click **Done**.

Defining a manual key

Follow these steps to define a manual key:

1 Select Automatic (IKE) from the **Key Management** drop list.

2 Click the **Manual Key**.
The New Manual Key dialog box appears.



New Manual Key

☑ ESP

Local SPI: Peer SPI:

Encryption Algorithm: 3DES

Encryption Key:
● String ○ Hex
Key:
Confirm Key:

Authentication Algorithm: MD5

Authentication Key:
● String ○ Hex
Key:
Confirm Key:

□ AH

Local SPI: Peer SPI:

Authentication Algorithm: MD5

Authentication Key:
● String ○ Hex
Key:
Confirm Key:

You can configure the manual key to use ESP (Encapsulated Security Payload), AH (Authenticated Headers), or both.

1 Enable the **ESP** checkbox.

2 Type a unique number between 256 and 65535 in the **Local SPI** (Security Parameter Index) field.
This SPI entry is used to identify this manual key in the local Firebox Vclass appliance.

3 Type the unique number of the remote appliance in the **Peer SPI** field.

4 Select the **Encryption Algorithm** from the drop list.

5 Select either **String** or **Hex for the Encryption Key** to specify the key text to be used, either character or hexadecimal notation.

6 Type and confirm the key in the appropriate fields.

7 Select the **Authentication Algorithm** from the drop list.

8 Select either **String** or **Hex for the Authentication Key** to specify the key text to be used, either character or hexadecimal notation.

9 Type and confirm the key in the appropriate fields.

10 Click to select the **AH** checkbox.

11 Type a unique number between 256 and 65535 in the **Local SPI** (Security Parameter Index) field.

This SPI entry is used to identify this manual key in the local Firebox Vclass appliance.

12 Type the unique number of the remote appliance in the **Peer SPI** field.

NOTE

If both ESP and AH are activated for this manual key, the local SPI for both ESP and AH must share the same unique number. Similarly, the peer SPI of both ESP and AH must also share a unique number.

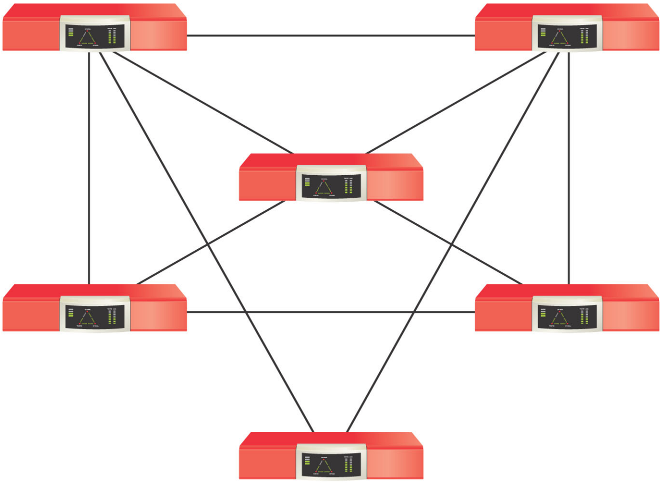
13 Select the **Authentication Algorithm** from the drop list.

14 Select either **String** or **Hex for the Authentication Key** to specify the key text to be used, either character or hexadecimal notation.

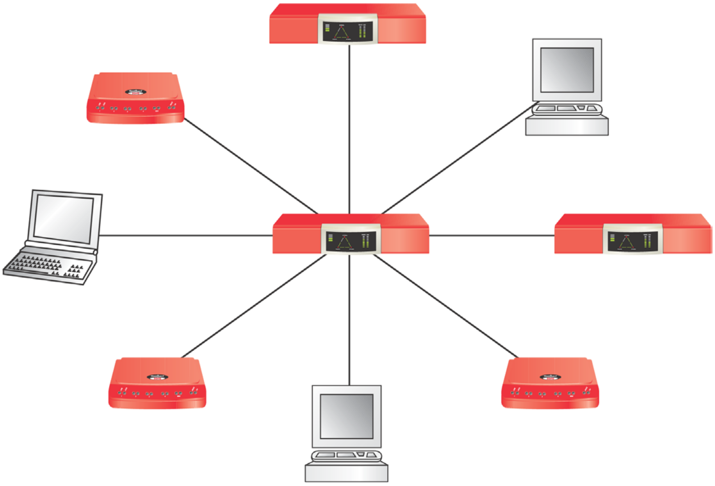
15 Type and confirm the key in the appropriate fields.

Using Tunnel Switching

Maintaining and managing VPN tunnels can be complicated and labor-intensive. This is particularly true when using a *fully meshed* topology in which a VPN tunnel is created between all sites. As the number of VPN sites increases, managing and maintaining tunnels among all the sites becomes much more difficult. The situation gets even more complicated after remote users establish their own VPN connections to the corporate network and to branch offices. The following figure depicts a fully meshed configuration.



A more efficient way to manage a complex corporate VPN with numbers of sites and remote users is to use a hub-and-spoke configuration, in which all branch offices connect to corporate headquarters (or any centralized site) with a single VPN tunnel. All communications between branch offices pass through the designated central site. Remote users, too, can dial into headquarters to access branch offices without the need to establish additional VPN tunnels. This topology, shown in the following figure, dramatically reduces the effort of managing a VPN.



To make such a hub-and-spoke topology effective and efficient, Firebox Vclass security appliances provide *tunnel switching* capabilities. Such a setup means that Site A can communicate with site B by sending traffic to the central office, which then switches this traffic from one tunnel (site A / central office) to another tunnel (site B / central office). All tunnel switching is performed in the Firebox Vclass appliance, which prevents any degradation of network performance.

The greatest benefit gained from tunnel switching is the reduction in cost of managing corporate VPNs. If a new branch office is added to the corporate VPN network, the administrator only needs to add a new policy in the Firebox Vclass appliance at headquarters. No additional configuration is needed for the branch offices.

Before you enable tunnel switching, make sure you have:

- Certificates for both ends of the IKE exchange, if RSA or DSS authentication is used.
- Agreements on other exchange parameters.

NOTE

Tunnel switching is not available on the V10 model.

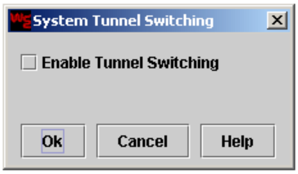
Enabling tunnel switching

Before you set up individual VPN policies for site-to-site tunnel switching, you must activate tunnel switching in the Firebox Vclass appliance hardware (which is disabled by default). To do so, follow these steps:

1 Open the Policy Manager window.

2 Click the **Tunnel Switch** button in the left margin.

The System Tunnel Switching dialog box appears.


System Tunnel Switching

□ Enable Tunnel Switching

3 Click the checkbox labeled **Enabled**.

4 Click **OK**.

CHAPTER 10

Creating a Remote User VPN Policy

With easy access to the Internet from home offices or on the road, employees and consultants are now able to connect to a corporate network from almost anywhere in the world. These connections require implementation of a VPN at corporate sites to guarantee the security of all data exchanges.

About Remote User VPNs

The Remote User VPN feature, also known as Remote Access Service (RAS), is built into every Firebox Vclass appliance and provides the following benefits:

- With proper policy configuration, users of remote VPN client connections must perform user-specific authentication, in addition to the regular computer-based authentication (using IKE phase one authentication).
- Internal IP addresses for VPN client use can be dynamically assigned to clients by Firebox Vclass appliances, which makes address management efficient and effective.
- Administrators can limit the duration of VPN client sessions and establish idle-timeout limits.

- Remote users can be associated with different user groups through which network administrators can establish group-wide parameters for all VPN client sessions, such as IP address assignment, session time limit, and idle timeout.
- A detailed remote user log is provided to the network administrator with information on all VPN client sessions. These logs now report on the times of user logon and logoff, where a user logs in from, which IP address is assigned to each user, and the amount of traffic generated by a user.
- A comprehensive monitor assists administrators in viewing the current list of VPN client sessions and detailed information on each client session. You can also use this monitor to disconnect active sessions.

The current implementation of the RAS VPN feature supports two different types of user authentication databases; the Firebox Vclass appliance's built-in user database (which you must configure) or an existing RADIUS server with current user records.

Requirements

Before creating a new remote user VPN policy, you need to do the following:

- Determine which user authentication database will be used—a database stored in a RADIUS server or an internal user database created and stored on a Firebox Vclass appliance.
- If you will be using a RADIUS server database, you'll need to know whether the authentication protocol is PAP or SecurID.
- If using a RADIUS database, you'll need the IP addresses of the primary and the backup RADIUS servers, if applicable.
- If you will be creating an internal-appliance database, you'll need to know each user's ID and password for inclusion in a user account.
- If a new IP address is going to be assigned to each remote user, determine the range of IP addresses that will be set aside for remote users. The set of IP addresses that will be applied to remote users should not include any that are currently assigned to existing network assets or users.

- To complete the VPN policy, you'll need to create the specific IKE policy that will be used by the remote access connections.
- Determine which areas or assets of a network will be made accessible to the users and which services will be permitted, including email, ftp, HTTP, and so on. In addition, you must provide Firebox Vclass VPN client software to external users, along with instructions for secure connections.

High-level view of remote user policies

This section presents a high-level view of how to create remote user policies. For specific procedures, see the subsequent sections.

1 Use the **RAS Configuration** dialog box to do the following:
   - Select the remote user validation from either an internal database or a RADIUS server
   - Create the user group profiles required
   - Add all the individual user accounts and link them to the appropriate group profiles

2 Use Policy Manager to create an IKE policy for user in remote user connections.

3 Use Policy Manager to create a VPN policy for remote access use.

To start with remote access configuration, decide which authentication database you want to use—Firebox Vclass-appliance internal or RADIUS—and see the appropriate section:

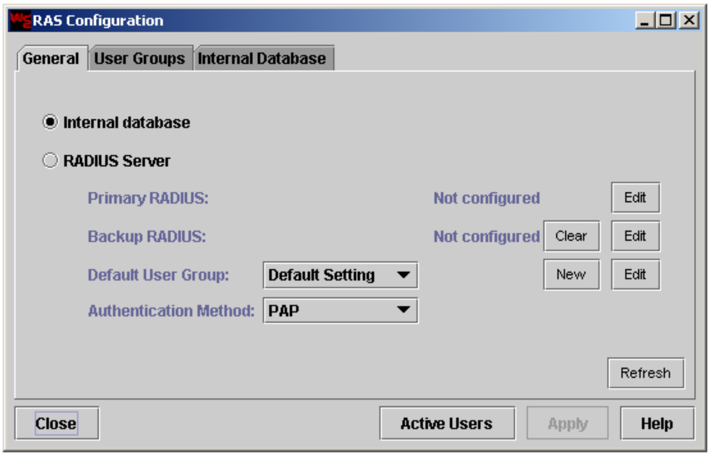
- "Configuring Remote Users" on page 201.
- "Using an internal authentication database" on page 204.

Configuring Remote Users

Before creating a VPN policy to manage remote user traffic, you must first choose the user authentication database your appliance will use. Next, if you want to use Vcontroller to assign internal IP addresses, you must set up the user group profiles required.

To configure remote users, first define a user group profile:

1 From the main Vcontroller page, click **Remote Users**.
The RAS Configuration dialog box appears.



RAS Configuration

● Internal database

○ RADIUS Server

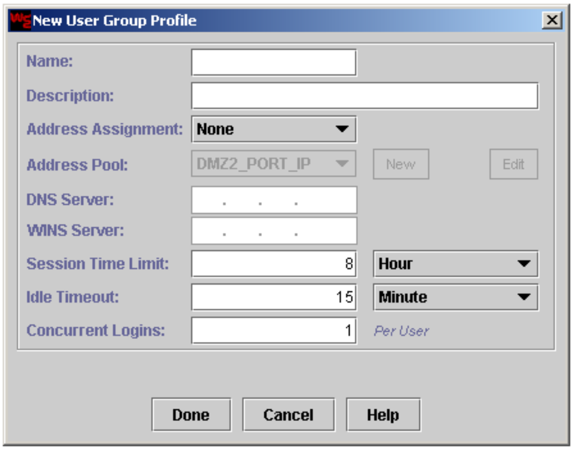
Primary RADIUS: Not configured

Backup RADIUS: Not configured

Default User Group: Default Setting

Authentication Method: PAP

2 To the right of the **Default User Group** drop list, click **New**.
The New User Group Profile dialog box appears.



New User Group Profile

Name:

Description:

Address Assignment: None

Address Pool: DMZ2_PORT_IP

DNS Server: . . .

WINS Server: . . .

Session Time Limit: 8 Hour

Idle Timeout: 15 Minute

Concurrent Logins: 1 *Per User*

3 Type a name and brief description for the user group in the appropriate fields. The **Description** field is optional.

4 Select one of the following options from the **Address Assignment** drop list:

None

Remote users belonging to this group will not be assigned an internal IP address when a connection is made.

Internal

Each remote user will be assigned an internal IP address when a connection is made. You must then select a preconfigured address group from the **Address Pool** drop list or click **New** to create a new address group. For information on creating an address group, see “Defining an address group” on page 126.

5 Type the IP address of the DNS server to be assigned to remote users in the **DNS Server** field.

6 Type the IP address of the WINS server to be assigned to remote users in the **WINS Server** field.

7 Type the appropriate number or hours or minutes until a user session expires in the **Session Time Limit** field.

8 Select either **Hours** or **Minutes** from the **Session Time Limit** drop list.

9 Type the appropriate number of hours or minutes in the **Idle Timeout** field.

10 Select either **Hours** or **Minutes from** the I**dle Timeout** drop list.

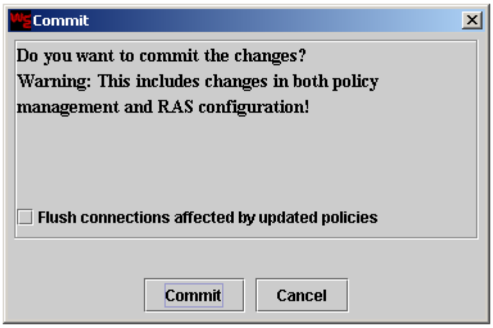
11 Type the maximum number of logins to be permitted in the **Concurrent Logins** field.

12 Click **Done**.

This new user group profile is displayed in the User Group entry list.

13 Click **Apply**.

The Commit dialog box appears.



Commit

Do you want to commit the changes?
Warning: This includes changes in both policy management and RAS configuration!

□ Flush connections affected by updated policies

14 To flush any active connections that may be affected by the changes, click the appropriate checkbox and then click **Commit**.

To continue configuring remote users, select an authentication method:

Internal database
For information on using this option to authenticate remote users, see “Using an internal authentication database,” below.

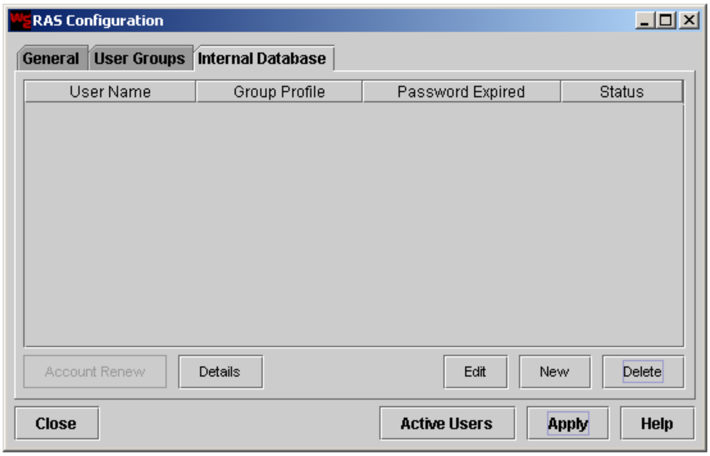
RADIUS Server
For information on using this option to authenticate Remote Users, see “Using a RADIUS authentication database” on page 206.

Using an internal authentication database

To set up an internal RAS user database, follow these steps:

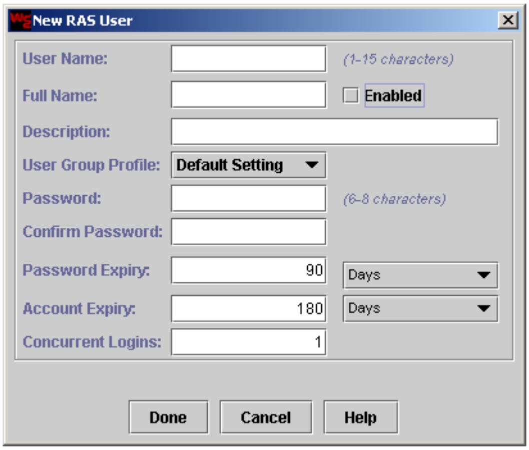
1 Enable the **Internal database** option.

2 Click the **Internal Database** tab.
The RAS users list is displayed.



User Name	Group Profile	Password Expired	Status

3 To create a new user entry, click **New**.
The New RAS User dialog box appears.


New RAS User

User Name: (1-15 characters)

Full Name: □ Enabled

Description:

User Group Profile: Default Setting

Password: (6-8 characters)

Confirm Password:

Password Expiry: 90 Days

Account Expiry: 180 Days

Concurrent Logins: 1

4 Type the **User Name** in the appropriate field.
User names are case-sensitive and must consist of 1 – 15 characters.

5 Type the full name of the RAS user and a brief description in the appropriate fields. The **Description** field is optional.

6 Select a user group profile from the drop list.

7 Type a password and confirm it in the appropriate fields.
Passwords are case-sensitive and consist of six to eight characters.

8 If you want, you can override the **Password Expiry**, **Account Expiry**, and **Concurrent Logins** default values to apply custom limitations to this account.

NOTE

The Enabled checkbox in the New RAS User dialog box controls whether or not this user account is active. If you need to temporarily disable an entry, select the user from the list of entries and click Edit. Click to clear the Enabled checkbox. You can reactivate this account at any time by clicking the Enabled checkbox again.

9 Click **Done**.
This entry is displayed among the RAS users entry list.

Repeat the previous steps to add other RAS users to the internal database.

10 When you are finished, click **Apply**.
The Commit dialog box appears.

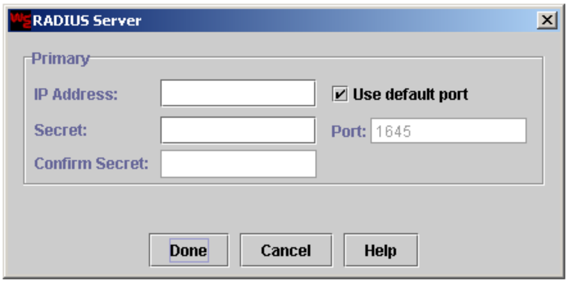
11. To flush any active connections that may be affected by the changes, click the appropriate checkbox and then click **Commit**.
12. To edit a RAS user entry, select the entry and click **Edit**.
13. To delete a RAS user entry, select the entry and click **Delete**.

Using a RADIUS authentication database

To use a database stored on a RADIUS server, follow these steps:

1. Enable the **RADIUS Server** option.
2. To the right of **Primary Radius**, click **Edit**.

   The RADIUS Server dialog box appears.



☑ Use default port

Port: 1645

3. Type the IP address of the RADIUS server in the **IP Address** field.
4. Type the secret and confirm it in the appropriate fields.
5. To change the port number, disable the checkbox labeled **Use default port**, and then type the number in the **Port** field.
6. Click **Done**.

   Repeat the previous steps to configure a connection to a backup RADIUS server.
7. Select either PAP or SecurID from the **Authentication Method** drop list.
8. Click **Done**.

   The IP address of the server is displayed.
9. Click **Apply**.

   The Commit dialog box appears.
10. To flush any active connections that may be affected by the changes, click the appropriate checkbox and then click **Commit**.

NOTE

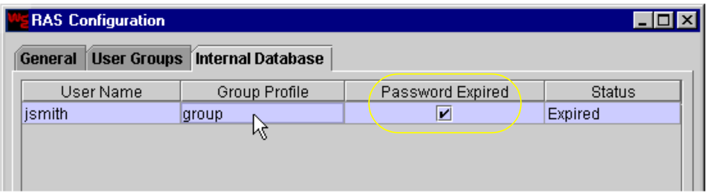
Depending on how the RADIUS servers area is configured, you might encounter a situation where the internal IP address and DNS server IP address information might be available on both the RADIUS server and the Firebox Vclass security appliance. In this case, the Firebox Vclass appliance automatically yields precedence to the RADIUS server when a user is being authenticated.

Resetting an expired password

After a remote user account password has expired, you can reset or replace it by following these steps:

1 Click the **Internal Database** tab.

Any users with expired passwords show a checkmark under the Password Expired column.



User Name	Group Profile	Password Expired	Status
jsmith	group	☑	Expired

2 Select the RAS user entry, and click **Edit**.

The Edit RAS User dialog box appears. The Password fields are inactive.

3 Click the checkbox labeled **Reset Password**.

The password fields become active.

4 Type a password and confirm it in the appropriate fields.

Passwords are case-sensitive and consist of six to eight characters.

5 Click **Done**.

6 Click **Apply**.

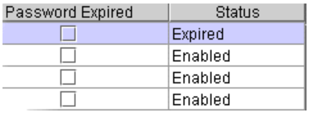
The Commit dialog box appears.

7 To flush any active connections that may be affected by the changes, click the appropriate checkbox and then click **Commit**.

Reactivating an expired user

After a remote user account has expired, you can reactivate it by resetting the account expiration.

1 Click the **Internal Database** tab.
  Any expired users are labeled as such under the Status column.



Password Expired	Status
☐	Expired
☐	Enabled
☐	Enabled
☐	Enabled

2 Select the expired user and then click **Account Renewal**.

3 Click **Done**.

4 Click **Apply**.
  The Commit dialog box appears.

5 To flush any active connections that may be affected by the changes, click the appropriate checkbox and then click **Commit**.

Editing and deleting a user group profile

If needed, you can reopen an existing user group profile and change any of the settings by selecting an existing user group profile and clicking **Edit**. Note, however, that if any address management parameters are changed (from None to Internal or vice versa), then all existing user connections belonging to this user group are disconnected. Any changes made to a policy are enforced immediately.

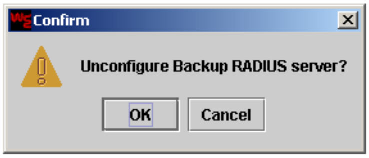
Similarly, if the address group used to store internal-use IP addresses is changed, then all user connections currently using IP addresses that are no longer valid are disconnected immediately. Note, however, that any change of default idle timeout does not affect existing user connections.

Removing the backup server

As described in "Configuring Remote Users" on page 201, you have the option to connect a Firebox Vclass appliance to both a primary and backup RADIUS server. The backup server may at some time become unavailable—temporarily or permanently. In this situation, you should remove the backup server setting.

1 From the main Vcontroller page, click **Remote Users**.
The RAS Configuration dialog box appears.

2 Click **Clear**, to the right of the backup RADIUS entry.
A confirmation window appears.



Confirm

Unconfigure Backup RADIUS server?

3 Click **OK**.
The Backup RADIUS status message reads "Not configured".

4 Click **Apply**.
The Commit dialog box appears.

5 To flush any active connections that may be affected by the changes, click the appropriate checkbox and then click **Commit**.

If the backup server is made available at a later time, you can repeat the process described in "Configuring Remote Users" on page 201 to re-establish the Firebox Vclass appliance connection to this server.

Defining a IKE and Security Policies for Remote Users

After you have decided which authentication database will be used and created any user group profiles required, you must define an IKE and Security policy that will be applied to the remote users. The process is the same as that of creating a other policies, but with these adjustments:

Observe these considerations when creating the security policies:

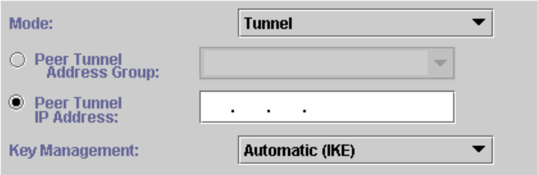
- If no internal IP addresses are to be assigned to remote users, the **Source** should be an address group with a membership of ANY.
- If, however, internal IP addresses will be automatically assigned to all remote users, the Source should then be the address group you created earlier in the **User Group Profile** dialog box.

- The **Destination** will be only those network resources accessible by remote access users.
- The **Services** will be limited to those that remote users will use, whether a few or a wide range of services.
- The **Incoming Interface** must be **0 (Public)**.

Form more information on configuring security policies, see “Defining a Security Policy” on page 125.

Observe these considerations when creating the IPSec action:

- You cannot specify a fixed IP address in the **Peer Tunnel IP Address** field. You should select this option, but leave the text field empty.



Mode: Tunnel

○ Peer Tunnel Address Group:

● Peer Tunnel IP Address: . . .

Key Management: Automatic (IKE)

- Select **Automatic (IKE)** from the **Key Management** drop list.

Form more information on configuring IPSec actions, see “Defining an IPSec action” on page 186.

Observe these considerations when creating the IKE policy:

- Because the remote clients can connect from anywhere on the Internet, the Peer Address Group *must* be set to ANY.
- Make sure this policy is listed below all other policies, at the bottom of the IKE Policy table. This will prevent the remote user policy from being applied to other policies.

Form more information on configuring IKE policies, see “Defining an IKE Policy” on page 180.

Observe this consideration when creating the IKE action:

- The **Extended Authentication** checkbox in the **New IKE Action** dialog box must be selected.

Form more information on configuring IKE policies, see “Defining an IKE action” on page 183.

Controlling a remote user's access privileges

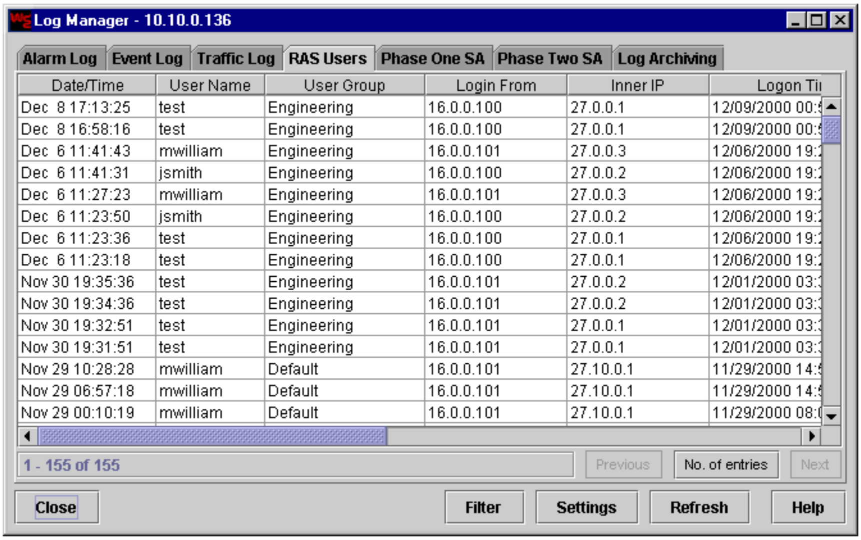
In addition to authenticating remote users, Firebox Vclass appliances can also be configured to assign a temporary internal IP address to a remote user. Typically, a remote user can be assigned to a specific user group. Each user group can be associated with an address group, which provides a pool of IP addresses for assignment.

After a remote user has been assigned an IP address, this address is subject to the security policies defined within the Policy Manager. Therefore, by controlling the network address assignment for a group of users, a network administrator can establish different levels of access privileges for whole groups of users.

Associating an address group to a user group allows you to control which part of the corporate networks can be accessed by users in a particular user group. This capability allows network administrators to set up different user groups for different levels of remote access.

Monitoring Remote User Activity

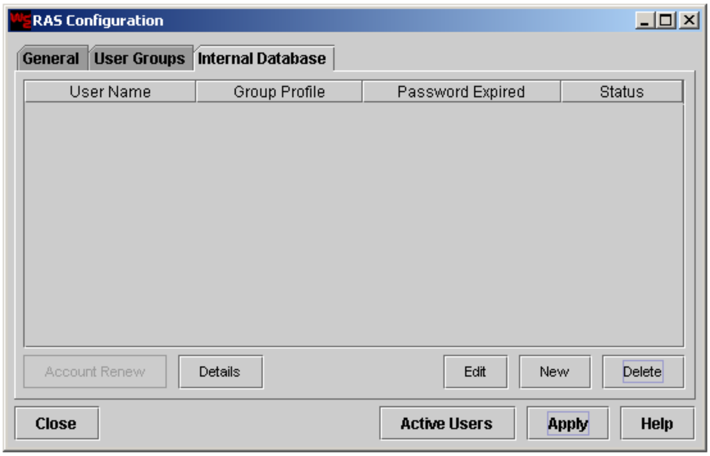
WatchGuard recommends that you take advantage of the Log Manager features. You can track and record remote access connections and system use.



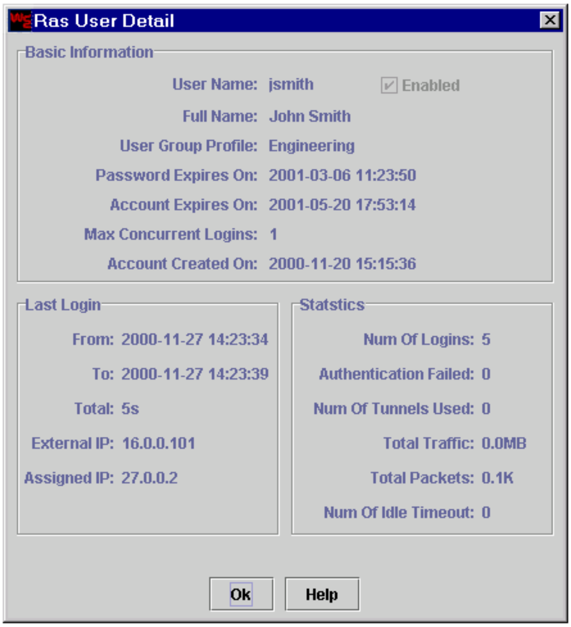
Date/Time	User Name	User Group	Login From	Inner IP	Logon Ti
Dec 8 17:13:25	test	Engineering	16.0.0.100	27.0.0.1	12/09/2000 00:
Dec 8 16:58:16	test	Engineering	16.0.0.100	27.0.0.1	12/09/2000 00:
Dec 6 11:41:43	mwilliam	Engineering	16.0.0.101	27.0.0.3	12/06/2000 19:
Dec 6 11:41:31	jsmith	Engineering	16.0.0.100	27.0.0.2	12/06/2000 19:
Dec 6 11:27:23	mwilliam	Engineering	16.0.0.101	27.0.0.3	12/06/2000 19:
Dec 6 11:23:50	jsmith	Engineering	16.0.0.100	27.0.0.2	12/06/2000 19:
Dec 6 11:23:36	test	Engineering	16.0.0.100	27.0.0.1	12/06/2000 19:
Dec 6 11:23:18	test	Engineering	16.0.0.100	27.0.0.1	12/06/2000 19:
Nov 30 19:35:36	test	Engineering	16.0.0.101	27.0.0.2	12/01/2000 03:
Nov 30 19:34:36	test	Engineering	16.0.0.101	27.0.0.2	12/01/2000 03:
Nov 30 19:32:51	test	Engineering	16.0.0.101	27.0.0.1	12/01/2000 03:
Nov 30 19:31:51	test	Engineering	16.0.0.101	27.0.0.1	12/01/2000 03:
Nov 29 10:28:28	mwilliam	Default	16.0.0.101	27.10.0.1	11/29/2000 14:
Nov 29 06:57:18	mwilliam	Default	16.0.0.101	27.10.0.1	11/29/2000 14:
Nov 29 00:10:19	mwilliam	Default	16.0.0.101	27.10.0.1	11/29/2000 08:

1 - 155 of 155

You can also get a basic summary of a particular user's recent connection history (not the current one) by opening the **RAS Configuration** dialog box's **Internal Database** tab, choosing a listed user, and clicking **Details**, as shown here.



A **RAS User Detail** dialog box appears, summarizing the most recent connection history of that user.



Basic Information

User Name: jsmith ☑ Enabled

Full Name: John Smith

User Group Profile: Engineering

Password Expires On: 2001-03-06 11:23:50

Account Expires On: 2001-05-20 17:53:14

Max Concurrent Logins: 1

Account Created On: 2000-11-20 15:15:36

Last Login

From: 2000-11-27 14:23:34

To: 2000-11-27 14:23:39

Total: 5s

External IP: 16.0.0.101

Assigned IP: 27.0.0.2

Statstics

Num Of Logins: 5

Authentication Failed: 0

Num Of Tunnels Used: 0

Total Traffic: 0.0MB

Total Packets: 0.1K

Num Of Idle Timeout: 0

- You can click **Active Users** to monitor currently active users.

  The System Information dialog box appears displaying a list of active RAS users. For more information on monitoring active RAS users, see "RAS User Information" on page 258.

CHAPTER 11

Monitoring the Firebox Vclass

For detailed status reports of the Firebox Vclass appliance you can use the Real-time Monitor.

You can activate the self-reporting capabilities by setting up and applying custom probes in the Real-time Monitor window. Then you can open the Real-time Chart window and watch the custom probes as they dynamically track the activities of the appliance and its network traffic.

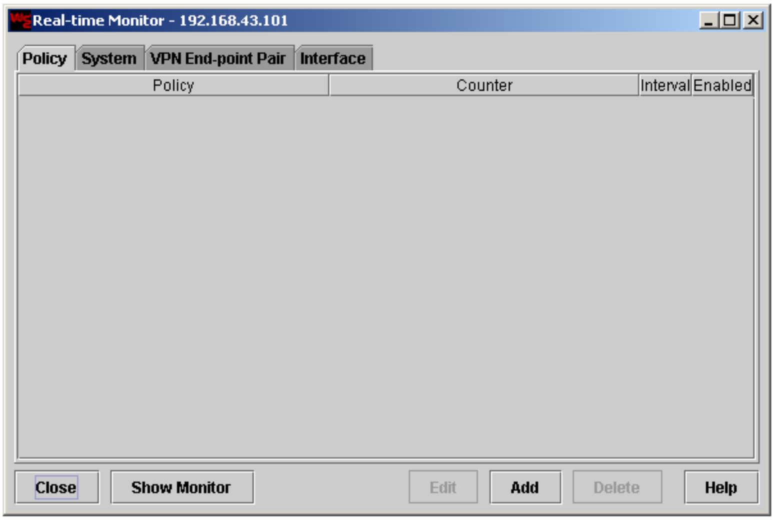
Using the Real-Time Monitor

A comprehensive system monitoring feature is available for your use in the Real-time Monitor window. This window provides a set of probes, which you can customize and apply, that generate real-time reports on usage of the system. The probes can then be viewed in a graphic display in the Real-time Chart window, which provides a visual “cardiogram” of the system’s health.

A real-time probe measures specific activity in a Firebox Vclass appliance, using counters to do so. To review a detailed catalog of available counters, see “A Catalog of Real-time Monitor Probe Counters” on page 220.

From the main Vcontroller page, click **Monitor**.

The Real-time Monitor window appears.



The following categories of system activity can be defined and monitored:

Policy

Policy probes observe and report on the activities of selected policies. For example, you can set up a probe to monitor the number of packets governed by a specific policy.

System

System probes provide snapshots of the operational status. For example, you can create separate probes that track both CPU and memory use, total throughput for the entire system, and amount of free space available for log files.

VPN End-point Pair

VPN End-point Pair probes report on specific encryption and authentication activity, as well as assessing traffic between a designated pair of security appliances. A “VPN End-point Pair” indicates a pair of appliances actively exchanging traffic through any number of IPSec tunnels, whether one or several.

Interface

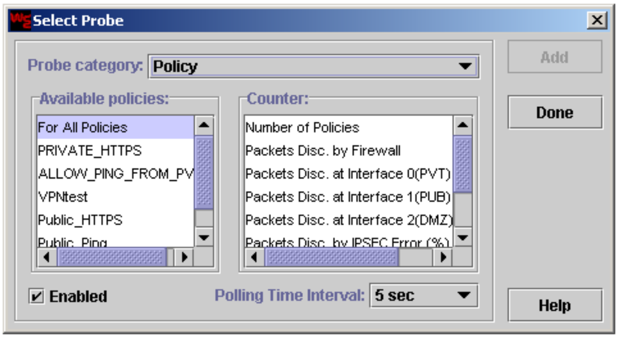
Interface probes observe and report on the activities of selected interfaces. For example, you can set up a probe to monitor the number of packets received by a specific interface.

Defining probes

To define a probe for any of the categories, follow these steps:

1 Click **Add**.

The Select Probe window appears.


Select Probe
Add
Done
Help
Available policies:
For All Policies
PRIVATE_HTTPS
ALLOW_PING_FROM_PV
VPNtest
Public_HTTPS
Public_Ping
Counter:
Number of Policies
Packets Disc. by Firewall
Packets Disc. at Interface 0(PVT)
Packets Disc. at Interface 1(PUB)
Packets Disc. at Interface 2(DMZ)
Packets Disc. by IPSEC Error (%)

Probe category: Policy

☑ Enabled

Polling Time Interval: 5 sec

2 From the **Probe Category** drop list, select a category.

After you select a probe category, the window refreshes and displays fields relevant to the category you select.

3 From the **Polling Time Interval** drop list, select an appropriate time interval for this probe. The range is between 5 and 60 seconds.

4 Click the checkbox labeled **Enabled** to active this probe as soon as you close the window. Otherwise, the probe will *not* be active.

A checkmark appears.

5 Click **Add** when you are finished configuring this probe.

The Select Probe window closes and the new probe is displayed in the appropriate tab list.

6 Repeat these steps to add more probes. Click **Done** when you are finished.

To edit the settings of an existing probe, follow these steps:

1 Select the probe. Click **Edit**.

2 When the **Select Counter** window appears, you can use its features to switch counters as needed. If you need to add a second counter to

monitor a specific policy, you may need to click **Add** to create an new probe.

3 When the probe has been edited, you can test it. Click **Show Monitor** (in the Real-time Monitor window) and then click **Start Monitoring** to activate the graphic display.

To disable an existing probe, follow these steps:

1 Click the tab for the probe you want to disable.

2 Click the checkbox on the right labeled **Enabled**.
The checkmark disappears. Disabling a probe is temporary; you can re-enable a probe at any time.

To delete an existing probe, follow these steps:

1 Click the relevant tab for the probe you want to delete.

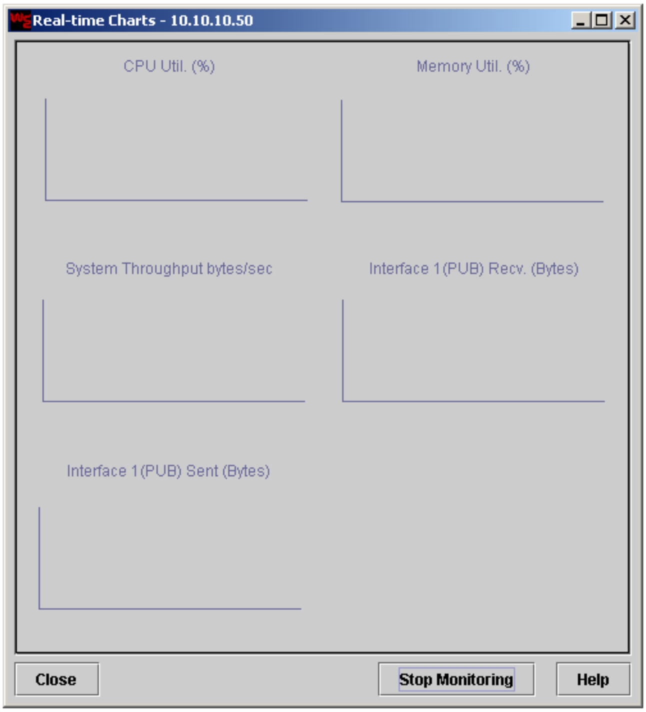
2 Select the probe you want to delete and then click **Delete**.

Monitoring configured probes

To view the actual level of activity of all the listed probes in one of the tabs, follow these steps:

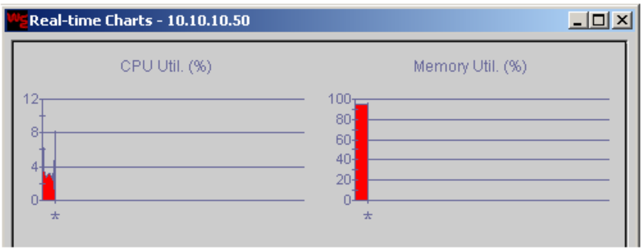
1 Click the tab for the probes you want to monitor.

2 Click **Show Monitor**.
The Real-time Charts window appears.


Real-time Charts - 10.10.10.50
CPU Util. (%)
Memory Util. (%)
System Throughput bytes/sec
Interface 1 (PUB) Recv. (Bytes)
Interface 1 (PUB) Sent (Bytes)
Close
Stop Monitoring
Help

3 Click **Start Monitoring**.

After a brief pause, which reflects the Interval times previously selected, the activity measured by each probe is displayed. The graph changes according to the per second interval you configured.



4 When you are finished monitoring, click **Stop Monitoring**.

5 Click **Close**.

To conserve system resources, you can temporarily disable any probes until the next time you want to monitor that particular system activity. At that time, you can re-enable the probe and observe the results in the Real-Time Chart window.

A Catalog of Real-time Monitor Probe Counters

System Counters

Counter Name	Function
CPU Util. (%)	System CPU utilization
Memory Util. (%)	System memory utilization
Interface 1(Public)Status (1=up)	Interface 1 status (1-up; 0-down)
Interface 0(Private)Status (1=up)	Interface 0 status (1-up; 0-down)
Interface 2(DMZ)Status (1=up)	Interface 2 status (1-up; 0-down)
System Throughput bytes/sec	Number of bytes processed per second
Packets Recv/sec	Packets received rate (packets/second)
Packets Sent/sec	Packets sent rate (packets/second)
IPSec Throughput bytes/sec	IPSec traffic throughput (bytes/sec)
IPSec Packets/sec	IPSec traffic throughput (packets/sec)
Total IPSec Tunnels	Total number of active IPSec tunnels
Interface 1(Public)Recv. (Bytes)	Number of bytes received from Interface 1 (bytes)
Interface 1(Public)Sent (Bytes)	Number of bytes sent from Interface 1 (bytes)

Counter Name	Function
Interface 1(Public)Recv. (Packets)	Number of packets received from Interface 1 (packets)
Interface 1(Public)Sent (Packets)	Number of packets sent from Interface 1 (packets)
Interface 1(Public)Recv Throughput, (Bytes/sec)	Rate of bytes received from Interface 1 (bytes/sec)
Interface 1(Public)Sent Throughput, (Bytes/sec)	Rate of bytes sent from Interface 1 (bytes/sec)
Interface 1(Public)Recv Throughput, (Packets/sec)	Rate of packets received from Interface 1 (packets/sec)
Interface 1(Public)Sent Throughput, (Packets/sec)	Rate of packets sent from Interface 1 (packets/sec)
Interface 0(Private) Received (Bytes)	Number of bytes received from Interface 0 (bytes)
Interface 0(Private) Sent (Bytes)	Number of bytes sent from Interface 0 (bytes)
Interface 0(Private) Recv. (Packets)	Number of packets received from Interface 0 (packets)
Interface 0(Private) Sent (Packets)	Number of packets sent from Interface 0 (packets)
Interface 0(Private) Recv. Throughput, (Bytes/sec)	Rate of bytes received from Interface 0 (bytes/sec)
Interface 0(Private) Sen Throughput, (Bytes/sec)	Rate of bytes sent from Interface 0 (bytes/sec)
Interface 0(Private) Recv. Throughput, (Packets/sec)	Rate of packets received from Interface 0 (packets/sec)
Interface 0(Private) Sent Throughput, (Packets/sec)	Rate of packets sent from Interface 0 (packets/sec)

Counter Name	Function
Interface 2(DMZ)Recv. (Bytes)	Number of bytes received from Interface 2 (bytes)
Interface 2(DMZ)Sent (Bytes)	Number of bytes sent from Interface 2 (bytes)
Interface 2(DMZ)Recv. (Packets)	Number of packets received from Interface 2 (packets)
Interface 2(DMZ)Sent (Packets)	Number of packets sent from Interface 2 (packets)
Interface 2(DMZ)Recv. Throughput, (Bytes/sec)	Rate of bytes received from Interface 2 (bytes/sec)
Interface 2(DMZ)Sent Throughput, (Bytes/sec)	Rate of bytes sent from Interface 2 (bytes/sec)
Interface 2(DMZ)Recv. Throughput, (Packets/sec)	Rate of packets received from Interface 2 (packets/sec)
Interface 2(DMZ)Sent Throughput, (Packets/sec)	Rate of packets sent from Interface 2 (packets/sec)
Log Disk Total (KB)	Total disk space for log files in Kbytes
Log Disk Used (KB)	Total disk space used for log files in Kbytes
Log Disk Free (KB)	Total disk space available for log files in Kbytes
Log Disk Used (%)	Percentage of disk space used for log files
Log Disk Free (%)	Percentage of disk space available for log files
Log Directory Size(KB)	Total size of the directory containing log files in Kbytes
Event Log Size (KB)	Event log file size in Kbytes

Counter Name	Function
Traffic Log Size (KB)	Traffic log file size in Kbytes
Alarm Log Size (KB)	Alarm log file size in Kbytes
Event Log Increment (KB)	Event log file size increment per interval
Traffic Log Increment (KB)	Traffic log file size increment per interval
Alarm Log Increment (KB)	Alarm log file size increment per interval
Event Log Growth Rate (KB/sec)	Event log file size increment rate (Kbytes/second)
Traffic Log Growth Rate (KB/sec)	Traffic log file size increment rate (Kbytes/second)
Alarm Log Growth Rate (KB/sec)	Alarm log file size increment rate (Kbytes/second)
Phase One SA Log Size (KB)	Phase one SA log file size in Kbytes
Phase Two SA Log Size (KB)	Phase two SA log file size in Kbytes
Remote User Log Size (KB)	Remote user log file size in Kbytes
Incoming Stream Requests	Number of incoming stream requests
Interface 1(Public) Stream Requests	Number of incoming stream requests from Interface 1
Interface 0(Private) Stream Requests	Number of incoming stream requests from Interface 0
Interface 2(DMZ) Stream Requests	Number of incoming stream requests from Interface 2
Incoming Stream Req./sec	Rate of incoming stream requests

Counter Name	Function
Interface 1(Public) Stream Req./sec	Rate of incoming stream requests from Interface 1
Interface 0(Private) Stream Req./sec	Rate of incoming stream requests from Interface 0
Interface 2(DMZ) Stream Req./sec	Rate of incoming stream requests from Interface 2
Incoming Stream Requests Denied	Number of denied stream requests
Interface 1(Public) Stream Requests Denied	Number of denied stream requests from Interface 1
Interface 0(Private) Stream Requests Denied	Number of denied stream requests from Interface 0
Interface 2(DMZ)Stream Requests Denied	Number of denied stream requests from Interface 2
Incoming Stream Req. Denied/sec	Rate of denied stream requests
Interface 1(Public)Stream Requests Denied/sec	Rate of denied stream requests from Interface 1
Interface 0(Private)Stream Requests Denied/sec	Rate of denied stream requests from Interface 0
Interface 2(DMZ)Stream Requests Denied/sec	Rate of denied stream requests from Interface 2
Total Bytes Recv.	Number of bytes received
Total Bytes Sent	Number of bytes sent
Total Packets Recv.	Number of packets received
Total Packets Sent.	Number of packets sent

Counter Name	Function
Total IPSEC Traffic (bytes)	IPSEC traffic in bytes
Total IPSEC Packets	IPSEC packets
Total Tunnel Mode SA	Number of tunnel mode SA in the system currently
Total Transport Mode SA	Number of transport mode SA in the system currently
Total ESP SA	Number of ESP protocol SA in the system currently
Total AH SA	Number of AH protocol SA in the system currently
Total Manual Key SA	Number of SA using manual key in the system currently
Total Auto Key SA	Number of SA using auto (IKE) key in the system currently
Total Expired SA	Total number of expired SA since start of system
HA1 Port Status (1=up)	HA1 interface status (1=up; 0=down)
HA2 Port Status (1=up)	HA2 interface status (1=up; 0=down)
Active User Sessions	Number of remote users' sessions
Remote Users Logon	Number of remote user logon's since last poll
Remote Users Logoff	Number of remote user logoff's since last poll
Remote Users Authentication Failed	Number of remote user logon's failed since last poll

Aggregate counters for all VPN end-point pairs

Counter Name	Description of Counter’s Function
Total Inbound SA	Total number of inbound SA
Total Outbound SA	Total number of outbound SA
Total SA	Total number of SA
Total Inbound Bytes/sec	Traffic rate through inbound SA
Total Outbound Bytes/sec	Traffic rate through outbound SA
Total Inbound Pkts/sec	Packet rate through inbound SA
Total Outbound Pkts/sec	Packet rate through outbound SA
Total Decryption Error Rate (%)	Total Decryption Error Packet Rate
Total Authentication Error Rate (%)	Total Authentication Error Packet Rate
Total Inbound SA	Total number of inbound SA

IPSec counters per VPN end-point pair

Counter Name	Description of Counter’s Function
Inbound SA	number of inbound SA of a VPN end-point pair
Outbound SA	number of outbound SA of a VPN end-point pair
Inbound Bytes/sec	Traffic rate through inbound SA of a VPN end-point pair
Outbound Bytes/sec	Traffic rate through outbound SA of a VPN end-point pair
Inbound Pkts/sec	Traffic rate through inbound SA of a VPN end-point pair

Counter Name	Description of Counter's Function
Outbound Pkts/sec	Traffic rate through outbound SA of a VPN end-point pair
Decryption Error Rate (%)	Decryption error packet rate of a VPN end-point pair
ESP Authentication Error Rate (%)	ESP authentication error packet rate of a VPN end-point pair
AH Authentication Error Rate (%)	AH authentication error packet rate of a VPN end-point pair
Replay Error Rate (%)	Replay error packet rate of a VPN end-point pair
Inbound Bytes	Number of inbound bytes of a VPN end-point pair
Outbound Bytes	Number of outbound bytes of a VPN end-point pair
Inbound Packets	Number of inbound packets of a VPN end-point pair
Outbound Packets	Number of outbound packets of a VPN end-point pair

Policy counters for all policies

Counter Name	Description of Counter's Function
Number of Policies	Total number of policies
Packets Disc. by Firewall	Total number of packets discarded by Firewall policies
Packets Disc. at Interface 1(Public)(%)	Percentage of packets discarded at Interface 1
Packets Disc. at Interface 0(Private)(%)	Percentage of packets discarded at Interface 0

Counter Name	Description of Counter's Function
Packets Disc. at Interface 2(DMZ)(%)	Percentage of packets discarded at Interface 2
Packets Disc. by IPSEC Error (%)	Percentage of packets discarded by IPSEC errors (decryption error, authentication error, replay error).
Packets Disc. by Decryption Error (%)	Percentage of packets discarded by Decryption errors
Packets Disc. by Authentication Error (%)	Percentage of packets discarded by Authentication errors
Packets Disc. by Replay Error (%)	Percentage of packets discarded by Replay errors

Policy counters per policy

Counter Name	Description of Counter's Function
Traffic (Bytes)	Number of bytes handled by a policy
Traffic (Packets)	Number of packets handled by a policy
Throughput (Bytes/sec)	Throughput in bytes/sec of a policy
Throughput (Pkts/sec)	Throughput packets/sec of a policy
Number of SA	Number of SA belongs to a policy
Packet Disc. (%)	Packet discarded rate of a policy
Decryption Error Packets	Number of packets handled by a policy with decryption error
Authentication Error Packets	Number of packets handled by a policy with authentication error
Replay Error Packets	Number of error packets handled by a policy with replay error.

Counter Name	Description of Counter’s Function
Decryption Error Rate (%)	Decryption error rate of a policy
Authentication Error Rate (%)	Authentication error rate of a policy
Replay Error Rate (%)	Replay error rate of a policy

CHAPTER 12

Using Alarm Manager

The Vcontroller Alarm Manager allows you to define alarms that can alert the appropriate parties when certain system or policy conditions occur.

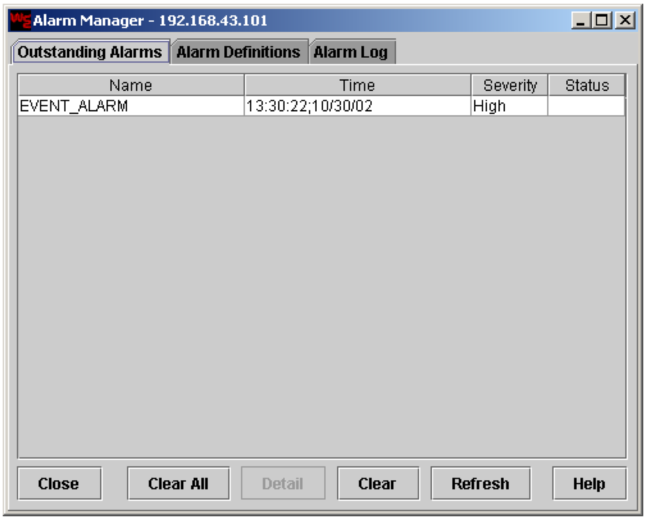
You can configure alarm notifications for basic system processes such as the log file reaching a certain size, or you can configure alarms that alert the on-duty system administrator when critical conditions have been detected. You can establish single-condition or multiple-condition alarms for any level of complexity that your system might encounter.

You can also use the Alarm Manager window to view the current status of the system and clear all current alarms that have been detected.

Alarm Definitions

To define a specific alarm condition, follow these steps:

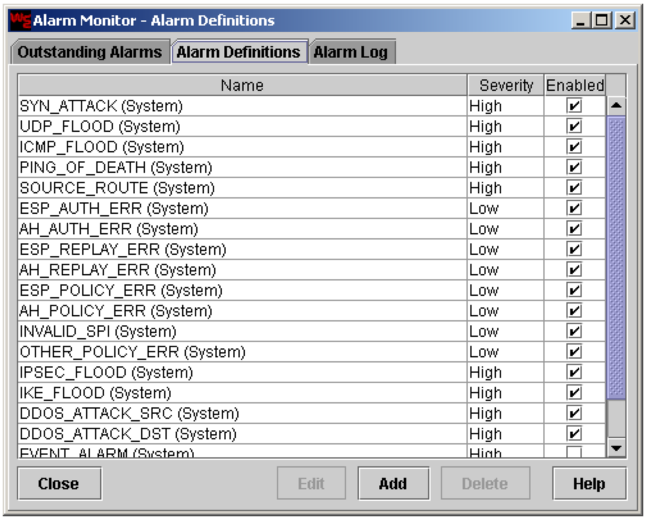
1 From the main Vcontroller page, click **Alarm**.
The Alarm Manager window appears.



Name	Time	Severity	Status
EVENT_ALARM	13:30:22;10/30/02	High	

2 Click the **Alarm Definitions** tab to view the current list of alarm definitions.

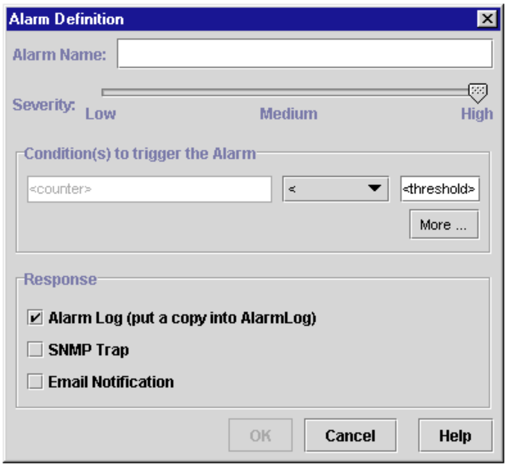
This tab lists pre-defined default alarms along with indications of their severity and whether or not they have been enabled.



Name	Severity	Enabled
SYN_ATTACK (System)	High	☑
UDP_FLOOD (System)	High	☑
ICMP_FLOOD (System)	High	☑
PING_OF_DEATH (System)	High	☑
SOURCE_ROUTE (System)	High	☑
ESP_AUTH_ERR (System)	Low	☑
AH_AUTH_ERR (System)	Low	☑
ESP_REPLAY_ERR (System)	Low	☑
AH_REPLAY_ERR (System)	Low	☑
ESP_POLICY_ERR (System)	Low	☑
AH_POLICY_ERR (System)	Low	☑
INVALID_SPI (System)	Low	☑
OTHER_POLICY_ERR (System)	Low	☑
IPSEC_FLOOD (System)	High	☑
IKE_FLOOD (System)	High	☑
DDOS_ATTACK_SRC (System)	High	☑
DDOS_ATTACK_DST (System)	High	☑
EVENT_ALARM (System)	High	□

3 Click **Add**.

The Alarm Definition dialog box appears.



☑ Alarm Log (put a copy into AlarmLog)

☐ SNMP Trap

☐ Email Notification

4 Type a name for the alarm in the appropriate field.

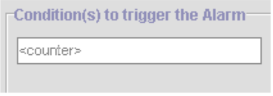
5 Click the **Severity** slider and move it to the point on the scale that matches the value of this alarm: **Low**, **Medium**, or **High**.

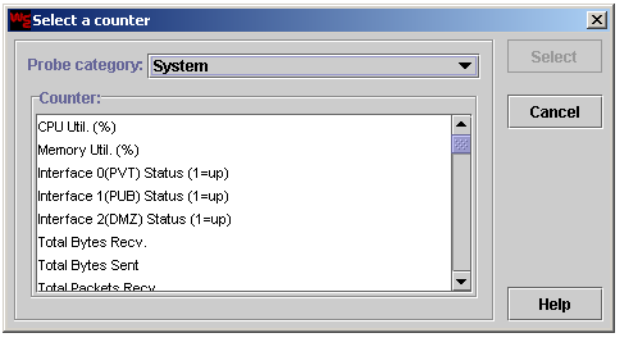
6 Decide whether the alarm will have more than one triggering condition.

Defining a single-condition alarm

1 Click the **Condition(s) to trigger the Alarm** field where <counter> appears. This field acts as a button.

The Select a Counter dialog box appears.




Select a counter

Probe category: System

Counter:

CPU Util. (%)
Memory Util. (%)
Interface 0(PVT) Status (1=up)
Interface 1(PUB) Status (1=up)
Interface 2(DMZ) Status (1=up)
Total Bytes Recv.
Total Bytes Sent
Total Packets Recv

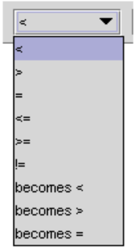
2. Select the appropriate option from the Probe Category drop list: **System**, **Policy**, or **VPN End-point Pairs**.
   The display changes depending upon your choice of Probe Category.

   Policy
   : Select the policy of your choice and then select the counter you want to use for the alarm. Selecting For All Policies displays a different list of counters.

   System
   : Select the counter you want to use for the alarm.

   VPN End-point Pairs
   : Select the IPSec pair of your choice and then select the counter you want to use for the alarm.

3. Click **Select.** For more information about the counters and their capabilities, see “A Catalog of Real-time Monitor Probe Counters” on page 220.
4. From the Alarm Definition window, select the option of your choice from the drop list.



<	Indicates "less than"
>	Indicates "greater than"
=	Indicates "equal to"
<=	Indicates "less than or equal to"
>=	Indicates "greater than or equal to"
!=	Indicates "not equal to becomes"
becomes >	Condition will be true if the counter value becomes greater than the threshold value
becomes <	Condition will be true if the counter value becomes less than the threshold value
becomes =	Condition will be true if the counter value becomes equal to the threshold value

5 Delete the text in the **<threshold>** field and type a number value for this counter. This value can be a whole number or a percentage.

6 To keep a record of all instances of this alarm, enable the **Alarm Log** response option.

7 To initiate an SNMP trap, enable the **SNMP Trap** response option. When this alarm is triggered, a message is sent to the Management Station.

8 To activate email notification, enable the **Email Notification** response option. Type the email address in the appropriate field. To send an email notification to more than one email address, type each address using a space to separate them.

9 Click **OK** when finished.

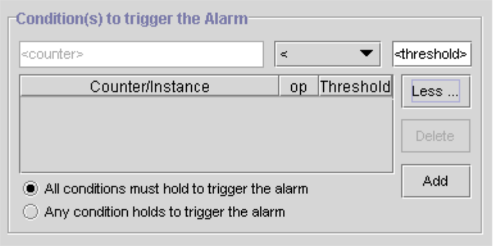
The new alarm definition appears in the list of Alarm Definitions. Repeat this process to create other single-condition alarms.

Defining a multiple-condition alarm

1 Click the **Alarm Definitions** tab and then click **Add**.

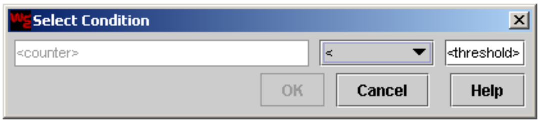
2 Click **More**.

Two condition options appear.



● All conditions must hold to trigger the alarm
○ Any condition holds to trigger the alarm

3 Click **Add**.
The Select Condition dialog box appears.



1 Click the text field where <counter> appears. This field acts as a button.
The Select a Counter dialog box appears.

2 Select the appropriate option from the Probe Category drop list: **System**, **Policy**, or **VPN End-point Pairs**.
The display changes depending upon your choice of Probe Category.

Policy
Select the policy of your choice and then select the counter you want to use for the alarm. Selecting For All Policies displays a different list of counters.

System
Select the counter you want to use for the alarm.

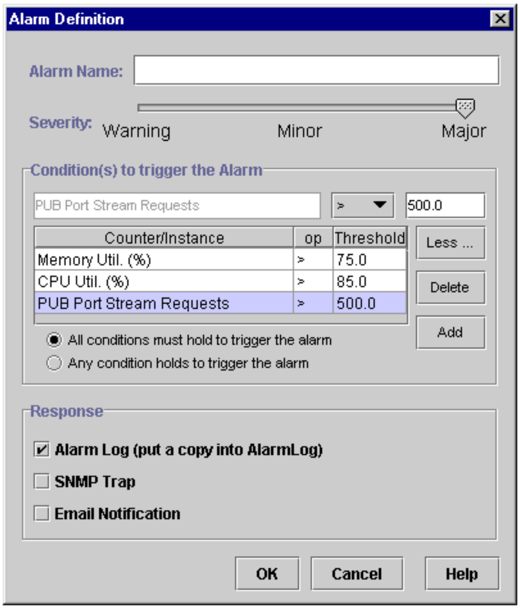
VPN End-point Pairs
Select the IPSec pair of your choice and then select the counter you want to use for the alarm.

3 Click **Select.** For more information about the counters and their capabilities, see “A Catalog of Real-time Monitor Probe Counters” on page 220.
The selected conditions appear in the Select Condition dialog box.

4 Select the appropriate option of your choice from the drop list.

5 Delete the text in the <threshold> field, type the value (either a whole number or a percentage) for this counter and then click **OK**.
The newly created condition appears in the Counter/Instance list.

6 Repeat this process to define more conditions for this specific alarm.
As a result, more than one condition will be listed in the Counter/Instance list



Alarm Definition

Alarm Name:

Severity: Warning Minor [✓ Major]

Condition(s) to trigger the Alarm

PUB Port Stream Requests | > | 500.0

Counter/Instance	op	Threshold
Memory Util. (%)	>	75.0
CPU Util. (%)	>	85.0
PUB Port Stream Requests	>	500.0

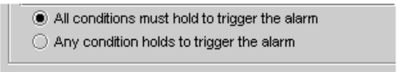
● All conditions must hold to trigger the alarm
○ Any condition holds to trigger the alarm

Response

☑ Alarm Log (put a copy into AlarmLog)
☐ SNMP Trap
☐ Email Notification

7 When you have completed your list of conditions, enable one of the two options:

- All conditions must hold to trigger the alarm
- Any condition holds to trigger the alarm

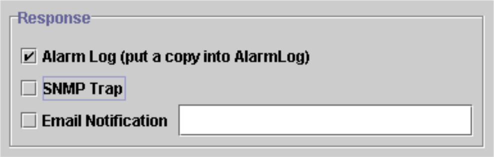


● All conditions must hold to trigger the alarm
○ Any condition holds to trigger the alarm

8 To keep a record of all instances of this alarm, enable the **Alarm Log** response option.

9 To initiate an SNMP trap, enable the **SNMP Trap** response option. When this alarm is triggered, a message is sent to the Management Station.

10 To activate email notification, enable the **Email Notification** response option. Type the email address in the appropriate field. To send an email notification to more than one email address, type multiple addresses separated by spaces.



☑ Alarm Log (put a copy into AlarmLog)

□ SNMP Trap

□ Email Notification

11 Click **OK** when finished.

The new alarm definition appears in the list of Alarm Definitions. Repeat this process to create other multi-condition alarms.

Managing alarm definitions

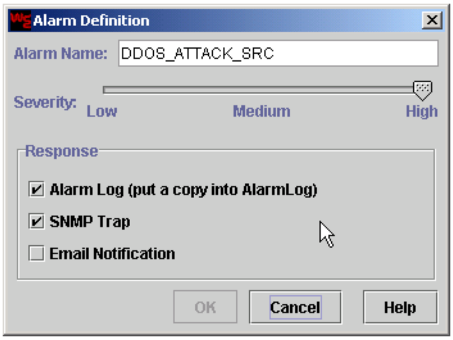
You can update an alarm definition, enable or disable a current alarm, or delete an alarm definition that is no longer needed in the Alarm Manager window.

To Update an alarm definition:

1 Open the Alarm Manager window. Click the **Alarm Definitions** tab.

2 Select the alarm that is to be updated and click **Edit**.

The Alarm Definition dialog box appears.



Alarm Name: DDOS_ATTACK_SRC

Severity: High

☑ Alarm Log (put a copy into AlarmLog)

☑ SNMP Trap

□ Email Notification

3 Make the changes to the severity and response options.

4 Click **OK** when finished to return to the Alarm Manager window.

5 Click **Close**.

To enable or disable an alarm:

1 Open the Alarm Manager window. Click the **Alarm Definitions** tab.

2 Locate the alarm to enable or disable. Enable or Disable the alarm by clicking the box.

3 Click **Close** when finished.

To delete an unwanted alarm definition:

1 Open the Alarm Manager window. Click the **Alarm Definitions** tab.

2 Select the alarm that to delete and click **Delete**.
The alarm definition is removed from the list.

3 Click **Close** when finished.

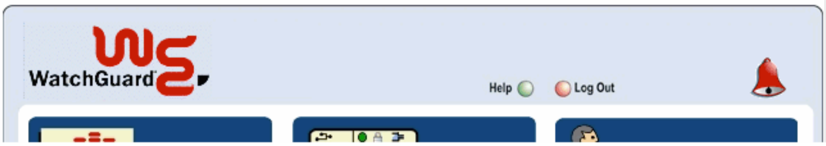
Responding to an Alarm Notification

Alarm notifications come in several forms:

- An animated alarm bell icon appears at the top of the WatchGuard Vcontroller main page.
- The red, Alarm LED illuminates on the front of the Firebox Vclass appliance.
- A notice appears in the Outstanding Alarms tab of the Alarm Manager window.
- You receive a SNMP trap message.
- You receive an email or pager notification.

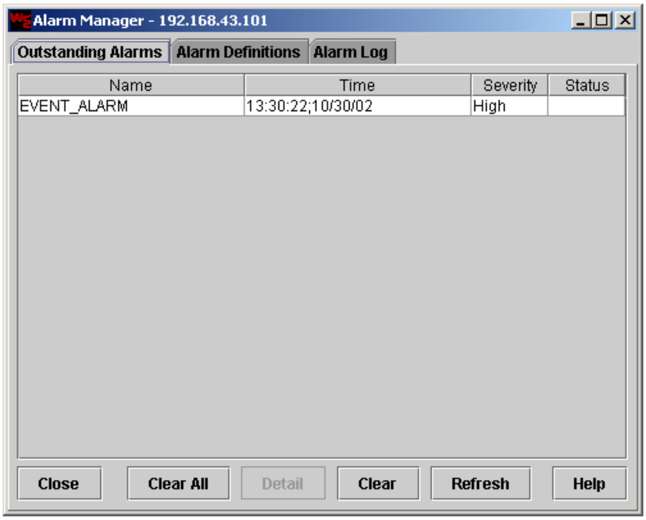
The relative severity of the alarm determines which contact method is used. If the alarm trigger is of a low severity, you may want to let the appliance display a notice in the Alarm Manager window and merely add it to the Alarm log. If, however, the alarm trigger is serious, you can configure the Firebox Vclass to add an SNMP trap or send an email notification.

In every alarm situation, the animated alarm bell appears in the upper-right corner of the Vcontroller main page to give administrators instant notice of a new alarm condition.



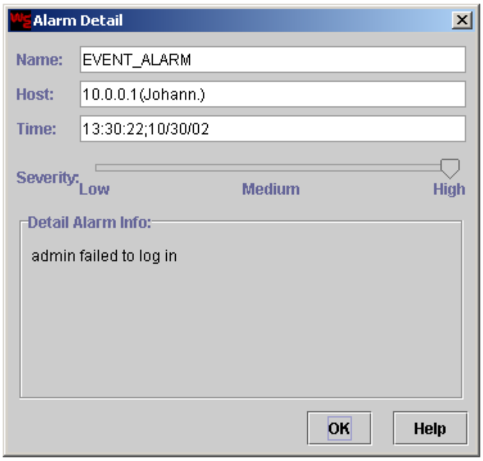
To view outstanding alarms:

1 From the Vcontroller main page, click the animated alarm bell or click the Alarm button.
The Alarm Manager window appears, listing the current alarms at the Outstanding Alarms tab.



Name	Time	Severity	Status
EVENT_ALARM	13:30:22;10/30/02	High	

2 Review the list of alarm notices. If you would like more information about a specific alarm notice, double-click the listing or select it and click **Detail**.
The Alarm Details dialog box appears.



Alarm Detail

Name: EVENT_ALARM

Host: 10.0.0.1(Johann.)

Time: 13:30:22;10/30/02

Severity: High

Detail Alarm Info:

admin failed to log in

3 Review the information displayed. This includes important information such as time, date, severity, and conditions (the counter used in this alarm).

4 Click **OK** to close the **Alarm Detail** dialog box.

5 To clear an outstanding alarm, select the alarm notice and click **Clear**. To clear *all* outstanding alarms, click **Clear All**.

The Alarm Manager removes the alarm notice from the Outstanding Alarms tab.

CHAPTER 13

Using Log Manager

The Vcontroller can log an extensive array of system activities and save all logs into text files that can be preserved for future reference. You can activate logging to record the following categories of system activities:

Event log
Records all the events such as key negotiation activities, denial-of-service attacks, device failures, and administrative activities.

Traffic log
Records all the traffic going through the appliance, and whether or not this data is passed or blocked according to the current set of policies.

Alarm log
Records a history of all alarms that have been triggered by various events or occurrences.

RAS User log
Records a history of every RAS client connection made through this appliance, including user name, origin of the connection, when the user logged in (and out), and a summary of connection statistics.

Phase One SA and Phase Two SA logs
Records the creation and expiration histories for each phase of security associations pertaining to VPN tunnels established in the system.

A Firebox Vclass appliance has a limited file-storage capacity. Log files are limited to 200 kilobytes (200 KB), except the Traffic log, which can be as large as 1 megabyte (1 MB).

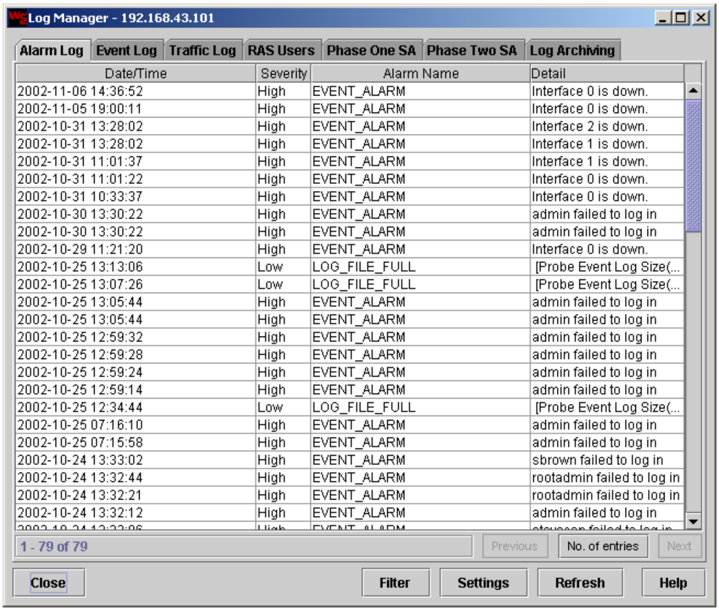
When a log file exceeds the preset limit, the oldest entries are deleted to make room for the most recent entries. To help you manage your log files to prevent losing any entries, a predefined alarm, “LOG_FILE_FULL,” alerts you when a specific log file is getting too big. At that time, you can back up the log file for future reference.

WatchGuard recommends the use of remote logging, using syslog, as described in “Activating the remote logging feature” on page 248.

Viewing the Logs

Use Log Manager to view your logs at any time. When the Log Manager window is opened, the Vcontroller contacts the Firebox Vclass appliance and extracts the latest logs. The 500 most recent entries are listed.

1 From the main Vcontroller page, click **Log Manager**.
The Log Manager window appears.



Date/Time	Severity	Alarm Name	Detail
2002-11-06 14:36:52	High	EVENT_ALARM	Interface 0 is down.
2002-11-05 19:00:11	High	EVENT_ALARM	Interface 0 is down.
2002-10-31 13:28:02	High	EVENT_ALARM	Interface 2 is down.
2002-10-31 13:28:02	High	EVENT_ALARM	Interface 1 is down.
2002-10-31 11:01:37	High	EVENT_ALARM	Interface 1 is down.
2002-10-31 11:01:22	High	EVENT_ALARM	Interface 0 is down.
2002-10-31 10:33:37	High	EVENT_ALARM	Interface 0 is down.
2002-10-30 13:30:22	High	EVENT_ALARM	admin failed to log in
2002-10-30 13:30:22	High	EVENT_ALARM	admin failed to log in
2002-10-29 11:21:20	High	EVENT_ALARM	Interface 0 is down.
2002-10-25 13:13:06	Low	LOG_FILE_FULL	[Probe Event Log Size(...
2002-10-25 13:07:26	Low	LOG_FILE_FULL	[Probe Event Log Size(...
2002-10-25 13:05:44	High	EVENT_ALARM	admin failed to log in
2002-10-25 13:05:44	High	EVENT_ALARM	admin failed to log in
2002-10-25 12:59:32	High	EVENT_ALARM	admin failed to log in
2002-10-25 12:59:28	High	EVENT_ALARM	admin failed to log in
2002-10-25 12:59:24	High	EVENT_ALARM	admin failed to log in
2002-10-25 12:59:14	High	EVENT_ALARM	admin failed to log in
2002-10-25 12:34:44	Low	LOG_FILE_FULL	[Probe Event Log Size(...
2002-10-25 07:16:10	High	EVENT_ALARM	admin failed to log in
2002-10-25 07:15:58	High	EVENT_ALARM	admin failed to log in
2002-10-24 13:33:02	High	EVENT_ALARM	sbrown failed to log in
2002-10-24 13:32:44	High	EVENT_ALARM	rootadmin failed to log in
2002-10-24 13:32:21	High	EVENT_ALARM	rootadmin failed to log in
2002-10-24 13:32:12	High	EVENT_ALARM	admin failed to log in

1 - 79 of 79

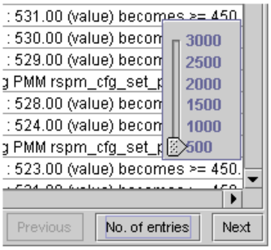
2 Click each tab to review the entries for that category.

3 If the log has more than 500 entries, as noted in the status message in the lower-left corner, click **Next** to download the next group of records.

4 Click **Prev** to display earlier listings.

5 To update the screen with the latest entries, click **Refresh**.

6 To increase or decrease the number of entries displayed, click **Number of Entries** in the lower-right corner of this window.
A counter pop-up appears in the tab.



```
: 531.00 (value) becomes >= 450
: 530.00 (value) becom
: 529.00 (value) becom
g PMM rspm_cfg_set_p
: 528.00 (value) becom
: 524.00 (value) becom
g PMM rspm_cfg_set_p
: 523.00 (value) becomes >= 450.
```

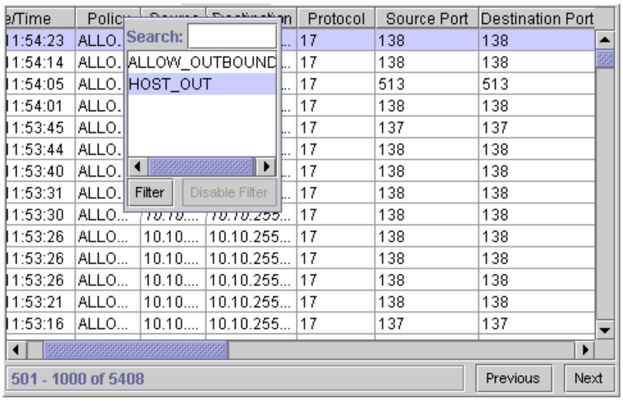
- Move the slider to the desired number and then click outside of the pop-up to close it.

Filtering a current log

When viewing a log, you may see a lot of entries you consider to be irrelevant. You can use the Filter feature to view only those activities or reports that you want to see.

1 After selecting the appropriate tab, right-click a specific column header to open the **Filter** pop-up window.

Right-clicking different column headers displays different filter choices relevant to the header.



e/Time	Polic	Source	Destination	Protocol	Source Port	Destination Port
11:54:23	ALLO.		...	17	138	138
11:54:14	ALLO.		...	17	138	138
11:54:05	ALLO.		...	17	513	513
11:54:01	ALLO.		...	17	138	138
11:53:45	ALLO.		...	17	137	137
11:53:44	ALLO.		...	17	138	138
11:53:40	ALLO.		...	17	138	138
11:53:31	ALLO.		...	17	138	138
11:53:30	ALLO...	10.10....	10.10.255...	17	138	138
11:53:26	ALLO...	10.10....	10.10.255...	17	138	138
11:53:26	ALLO...	10.10....	10.10.255...	17	138	138
11:53:26	ALLO...	10.10....	10.10.255...	17	138	138
11:53:21	ALLO...	10.10....	10.10.255...	17	138	138
11:53:16	ALLO...	10.10....	10.10.255...	17	137	137

2 Select a search option or type a text string in the Search field and then click **Filter**. You can use shift+select for more than one search option.

Vcontroller filters out only those records matching the search options and displays them in the tab. The column header you filtered displays an asterisk to the left of the title.

NOTE

Following a filtering action, you can right-click other column headings and repeat this process to further filter the entries until you have the exact records that you want.

3 To undo the filtering, reopen the **Filter** pop-up and click **Disable Filter.**

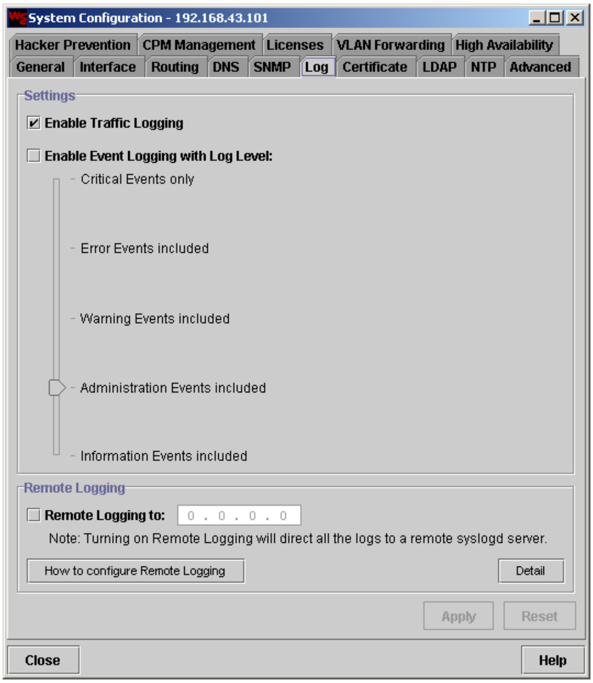
Vcontroller restores the previously visible log entries that were filtered out of view.

Log Settings

You can use four separate log files to monitor and record almost any level of Firebox Vclass system activities.

To configure the logging settings, follow these steps:

1 Click **Settings**.
The System Configuration dialog box appears displaying the log settings.



Settings

☑ Enable Traffic Logging

☐ Enable Event Logging with Log Level:

- Critical Events only
- Error Events included
- Warning Events included
- Administration Events included
- Information Events included

Remote Logging

☐ Remote Logging to: 0 . 0 . 0 . 0

Note: Turning on Remote Logging will direct all the logs to a remote syslogd server.

How to configure Remote Logging | Detail

2 To enable the Traffic log, click the checkbox labeled **Enable Traffic Log**.
The Firebox Vclass appliance begins logging traffic.

NOTE

If you leave this option disabled, you can still use the Log Manager window to view information about other system activity. For more information, see "Viewing the Logs" on page 244.

3 To enable the Event Log, click the checkbox labeled **Enable Event Logging**.

4 To change the amount of information recorded in the Event log, click the Event Log Level options slider and move it to the logging level you want.

NOTE

The system purges the oldest log files when they reach a certain size. The more events you include, the more frequently the log content is deleted. The Vcontroller provides a default alarm that notifies you when a log file is almost full.

Activating the remote logging feature

If you have a syslog server accessible through the network, you can designate that server as the default destination for all future log archive files. This is the preferred method for storing log files.

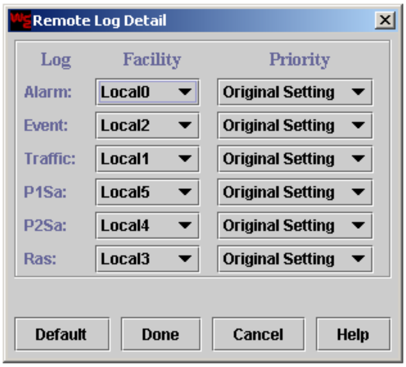
The Firebox Vclass appliance can record all the event, alarm, RAS user, phase one and phase two SA, and traffic logs to any designated remote server that supports the remote syslog mechanism. To make this possible, the remote logging features on the Firebox Vclass appliance must be linked to the log server, as described in the following instructions. In addition, the syslog daemon process on the server must be set to enable log traffic from other systems. The user documentation for the server should provide information on configuring such a link.

To store your log files on a remote server, follow these steps:

1 Click the checkbox labeled **Remote Logging**.

2 Type the IP address of the syslog server in the appropriate field.

3 Click **Detail**.
The Remote Log Detail dialog box appears.



Log	Facility	Priority
Alarm:	Local0	Original Setting
Event:	Local2	Original Setting
Traffic:	Local1	Original Setting
P1Sa:	Local5	Original Setting
P2Sa:	Local4	Original Setting
Ras:	Local3	Original Setting

4 Select the **Facility** and **Priority** from the drop lists for each log category. To use the default settings, click **Default**.

5 Click **Done**.

When you have finished configuring the logging settings, click one of the following options:

Reset
To return the settings to the previous configuration.

Apply
To immediately commit the settings to the Firebox Vclass appliance.

When you are finished, click **Close**.

The System Configuration dialog box closes.

Log Archiving

When your log files are sufficiently full, or if your organizational archiving policy dictates, you can archive your log files to a text file. This file will be archived to a specific directory on your workstation:

Windows workstations:
`c:\rs\log`

UNIX workstations:
users home directory

Log files are assigned a name in this format:

```
<type>_<date>.rsl
```

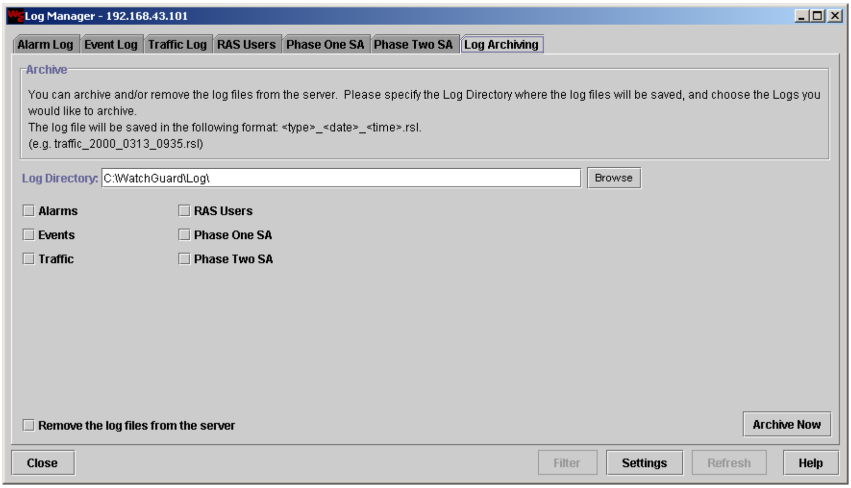
For example, a traffic log file that was archived at 10:30 am on May 19, 2001 would be named:

```
traffic_20010519_1030.rsl
```

To archive your log files, follow these steps:

1 From the main Vcontroller page, click **Log Manager**.
The Log Manager window appears.

2 Click the **Log Archiving** tab.



You can archive and/or remove the log files from the server. Please specify the Log Directory where the log files will be saved, and choose the Logs you would like to archive.
The log file will be saved in the following format: <type>_<date>_<time>.rsl.
(e.g. traffic_2000_0313_0935.rsl)

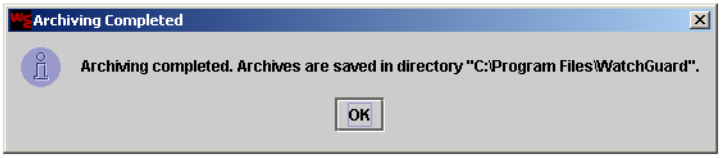
Log Directory: C:\WatchGuard\Log\

□ Alarms □ RAS Users
□ Events □ Phase One SA
□ Traffic □ Phase Two SA

□ Remove the log files from the server

3 Click the checkboxes—**Alarms**, **Events**, **Traffic, RAS Users, Phase One SA,** and **Phase Two SA**—to select the log category to archive.

4 Click **Archive Now** to archive a file to the default directory location: `C:\WatchGuard\Log\` or click **Browse** to select a different directory. When the archiving is complete, a dialog box appears.



Archiving completed. Archives are saved in directory "C:\Program Files\WatchGuard".

5 Click **OK**.

NOTE

You cannot set up the Firebox Vclass appliance to automatically archive logs.

CHAPTER 14

System Information

The **System Information** dialog box provides accurate and up-to-date information on your system's current status. This dialog box contains a number of tabs that provide information on a variety of system components.

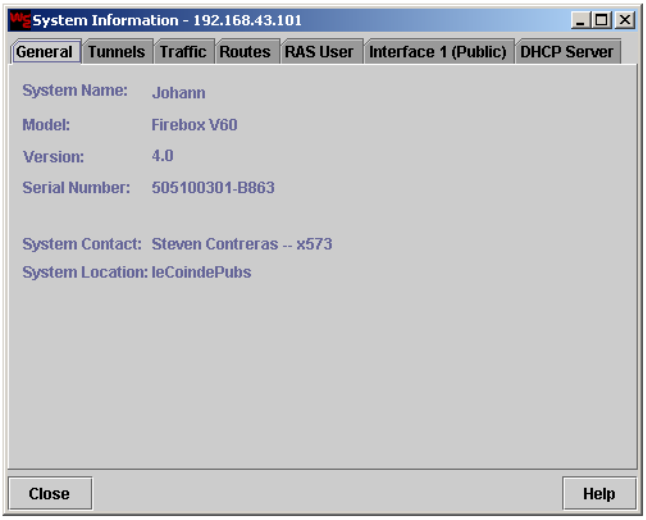
General Information

For general information on Firebox Vclass appliance status, use the **System Information** dialog box's **General** tab.

1 From the main Vcontroller page, click **System Information**.

The System Information dialog box appears.

2 Click the **General** tab.



System Name: Johann

Model: Firebox V60

Version: 4.0

Serial Number: 505100301-B863

System Contact: Steven Contreras -- x573

System Location: leCoindePubs

This tab allows you to access some general information, such as the model number, current system software version, serial number, contact person, and location of the appliance.

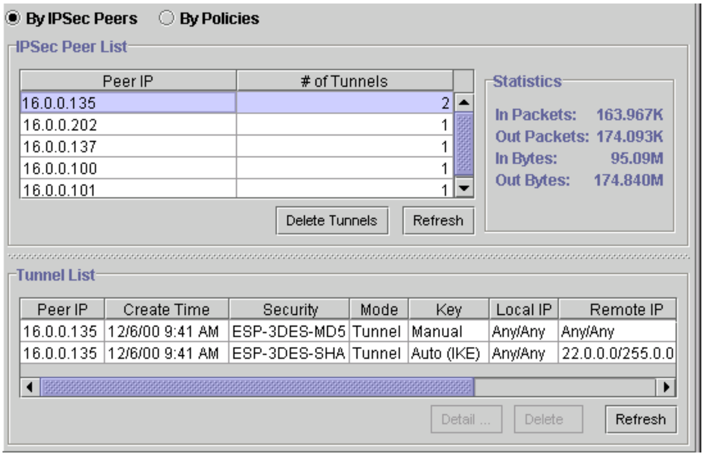
3 When you are finished, click **Close**.

VPN Tunnel Information

You can view tunnels and traffic statistics, delete specific tunnels, or delete all tunnels and purge the appliance of all residual tunnel records. Remember that tunnels are not always closed when the connection is broken.

- From the main Vcontroller page, click **System Information**.
  The System Information dialog box appears.
- Click the **Tunnels** tab.
- Click one of the following two display categories:

By IPSec Peers
Displays a list of currently active IPSec peers. The total count of tunnels may include some that are not in active use, but are still on record within the database.



Peer IP	# of Tunnels
16.0.0.135	2
16.0.0.202	1
16.0.0.137	1
16.0.0.100	1
16.0.0.101	1

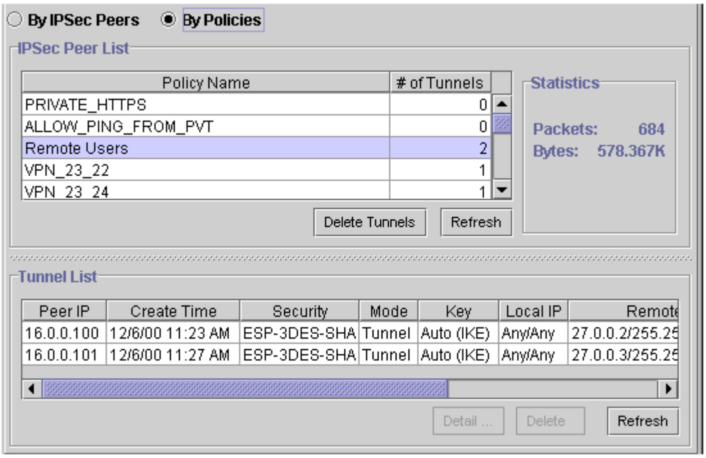
Statistics

In Packets:	163.967K
Out Packets:	174.093K
In Bytes:	95.09M
Out Bytes:	174.840M

Peer IP	Create Time	Security	Mode	Key	Local IP	Remote IP
16.0.0.135	12/6/00 9:41 AM	ESP-3DES-MD5	Tunnel	Manual	Any/Any	Any/Any
16.0.0.135	12/6/00 9:41 AM	ESP-3DES-SHA	Tunnel	Auto (IKE)	Any/Any	22.0.0.0/255.0.0

By Policies

Displays a list of all policies you have created and the number of VPN tunnels established by each policy.



Policy Name	# of Tunnels
PRIVATE_HTTPS	0
ALLOW_PING_FROM_PVT	0
Remote Users	2
VPN_23_22	1
VPN_23_24	1

Statistics

Packets:	684
Bytes:	578.367K

Peer IP	Create Time	Security	Mode	Key	Local IP	Remote
16.0.0.100	12/6/00 11:23 AM	ESP-3DES-SHA	Tunnel	Auto (IKE)	Any/Any	27.0.0.2/255.25
16.0.0.101	12/6/00 11:27 AM	ESP-3DES-SHA	Tunnel	Auto (IKE)	Any/Any	27.0.0.3/255.25

- to view the traffic statistics and the associated tunnels for a particular IPSec peer or policy, select the entry from the IPSec Peer list.

  The display refreshes and the statistics are displayed on the right. if there are any tunnels associated with this entry, the tunnel list displays them.

- Click **Delete Tunnels** to remove all established tunnels associated with this IPSec peer or policy and force the creation of new tunnels. If there are no established tunnels this button is unavailable.
- Click **Refresh** to remove the Statistics information from the IPSec Peer List field.
- To delete a specific tunnel associated with an IPSec Peer or Policy and force the creation of a new tunnel, select the entry from the tunnel list and click **Delete**.
- To update the tunnel list with the most recent information, click **Refresh**.
- When you are finished, click **Close**.

Viewing tunnel details

To view a detailed report of a specific tunnel, follow these steps:

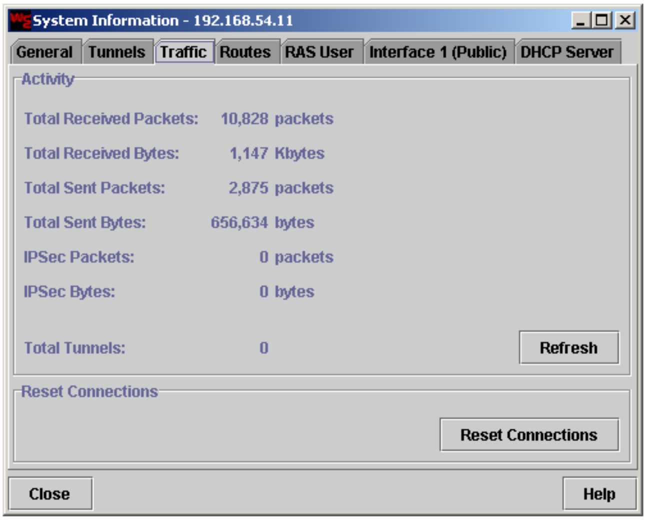
- Select an entry from the tunnel list and then click **Details**.
  The Detail Tunnel Information dialog box appears.
- Click **Refresh** to update the current SAs list with the most recent information. When you are finished, click **Close** to return to the **System Information** dialog box, **Tunnels** tab.

Traffic Information

To view traffic activity information, follow these steps:

- From the main Vcontroller page, click **System Information**.

  The **System Information** dialog box appears.
- Click the **Traffic** tab.



System Information - 192.168.54.11

Activity

Total Received Packets: 10,828 packets

Total Received Bytes: 1,147 Kbytes

Total Sent Packets: 2,875 packets

Total Sent Bytes: 656,634 bytes

IPSec Packets: 0 packets

IPSec Bytes: 0 bytes

Total Tunnels: 0

Reset Connections

The following information is displayed on the **Traffic** tab:

Total Packets
Total number of packets processed since the last reboot of this appliance. This includes packets that pass through this appliance and those that are discarded by firewall policies.

Total Bytes
Data traffic in total bytes processed through this appliance since the last reboot.

IPSec Packets
IPSec activity in total number of packets that have been encrypted or decrypted, since the last system startup.

IPSec Bytes
IPSec encryption/decryption activity in bytes.

Total Tunnels
Number of VPN tunnels.

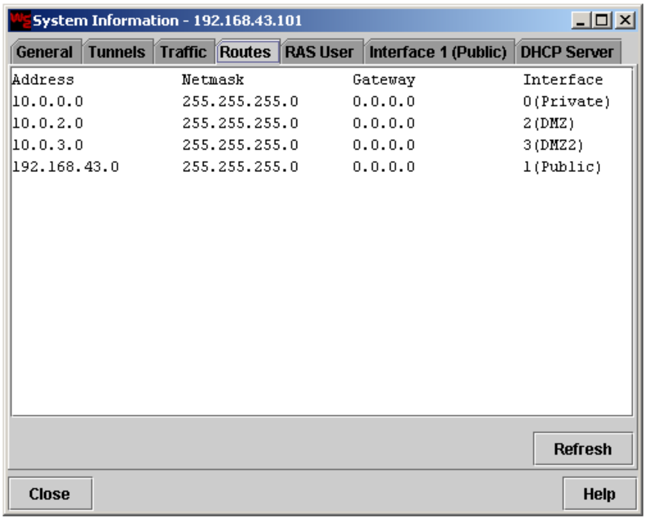
- Click **Refresh** to update the display with the most recent information.
- Click **Reset Connections** to disconnect all current connections. This will flush the Firebox Vclass appliance of all residual data connections that may be hampering performance.

- When you are finished, click **Close**.

Route Information

To view the routing table information, follow these steps:

1 Click the **Routes** tab.



```
Address             Netmask             Gateway             Interface
10.0.0.0            255.255.255.0       0.0.0.0             0(Private)
10.0.2.0            255.255.255.0       0.0.0.0             2(DMZ)
10.0.3.0            255.255.255.0       0.0.0.0             3(DMZ2)
192.168.43.0        255.255.255.0       0.0.0.0             1(Public)
```

2 Click **Refresh** to update the display with the most recent information.

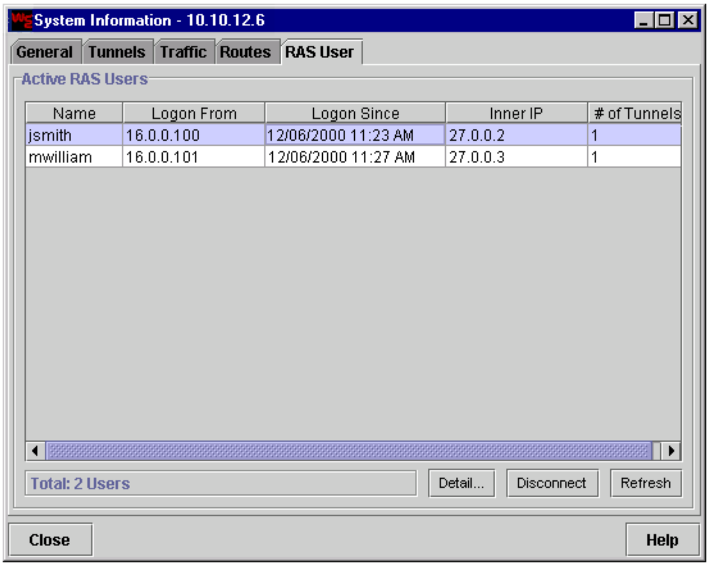
3 When you are finished, click **Close**.

RAS User Information

After you have set up Remote Access Service (RAS) and implemented VPN policies, you can monitor and manage the current remote user connections using the System Information window.

1 Click the **RAS User** tab.

This currently active RAS users are displayed.



Active RAS Users

Name	Logon From	Logon Since	Inner IP	# of Tunnels
jsmith	16.0.0.100	12/06/2000 11:23 AM	27.0.0.2	1
mwilliam	16.0.0.101	12/06/2000 11:27 AM	27.0.0.3	1

Total: 2 Users

2 Click **Disconnect** to break the selected user connection, including any established tunnels. If an internal IP address was assigned to this user, it will be returned to the system for future use.

3 Click **Refresh** to update the Active RAS Users display with the most recent information.

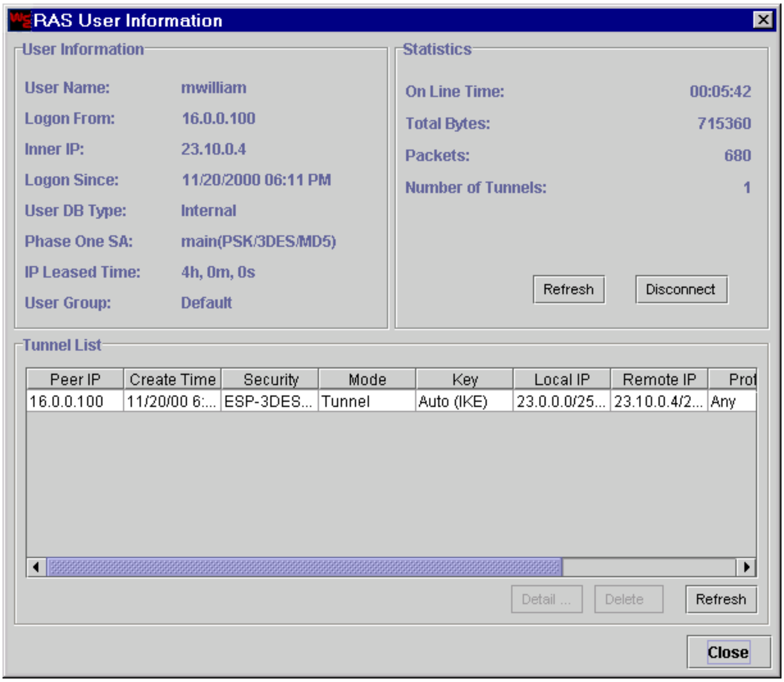
4 When you are finished, click **Close**.

Viewing RAS user information and tunnel details

You can view a real-time snapshot of a user connection, including information about the properties of a user, properties of tunnels being used by this user, and detailed traffic statistics.

1 Select a user entry from the Active RAS Users list and then click **Detail**.

The RAS User Information dialog box appears.



User Information

User Name: mwilliam
Logon From: 16.0.0.100
Inner IP: 23.10.0.4
Logon Since: 11/20/2000 06:11 PM
User DB Type: Internal
Phase One SA: main(PSK/3DES/MD5)
IP Leased Time: 4h, 0m, 0s
User Group: Default

Statistics

On Line Time: 00:05:42
Total Bytes: 715360
Packets: 680
Number of Tunnels: 1

Tunnel List

Peer IP	Create Time	Security	Mode	Key	Local IP	Remote IP	Prot
16.0.0.100	11/20/00 6:...	ESP-3DES...	Tunnel	Auto (IKE)	23.0.0.0/25...	23.10.0.4/2...	Any

The User Information and Statistics areas provide extensive information about this user and the current connection. The Tunnel List catalogs the tunnels currently in use.

2 Click **Refresh** to update the Statistics display with the most recent information.

3 Click **Disconnect** to break the selected user connection, including any established tunnels. If an internal IP address was assigned to this user, it will be returned to the system for future use.

4 To delete a specific tunnel associated with a RAS user and force the creation of a new tunnel, select the entry from the tunnel list and click **Delete**.

5 To update the tunnel list with the most recent information, click **Refresh**.

6 To view a detailed report of a specific tunnel, select an entry from the tunnel list and then click **Details**. Most of the time, a RAS User connection will have only a single tunnel.
The Detail Tunnel Information dialog box appears.

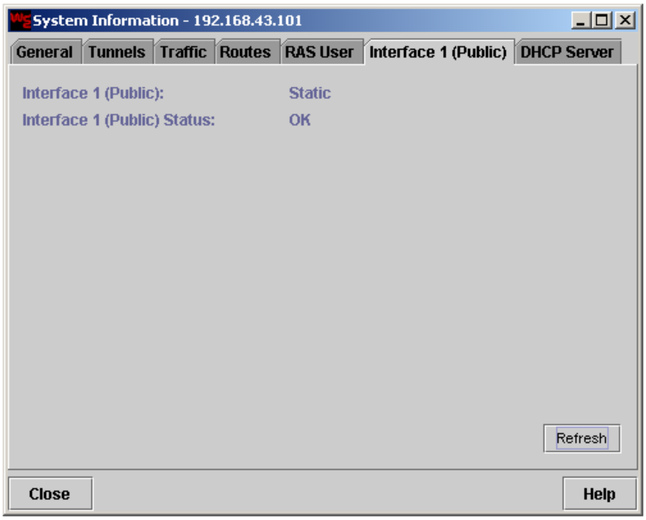
- Click **Refresh** to update the Current SAs list with the most recent information. When you are finished, click **Close** to return to the System Information, Tunnels tab.
- When you are finished, click **Close** to return to the RAS User Information window.

Interface 1 (Public) Information

This tab displays the status of interface 1 (Public) and the IP addressing mode in use—Static, DHCP, or PPPoE.

1 From the main Vcontroller page, click **System Information**.
The System Information dialog box appears.

2 Click the **Interface 1 (Public)** tab.
The Interface 1 (Public) information is displayed.



Interface 1 (Public): Static
Interface 1 (Public) Status: OK

3 Click **Refresh** to update the display with the most recent information.

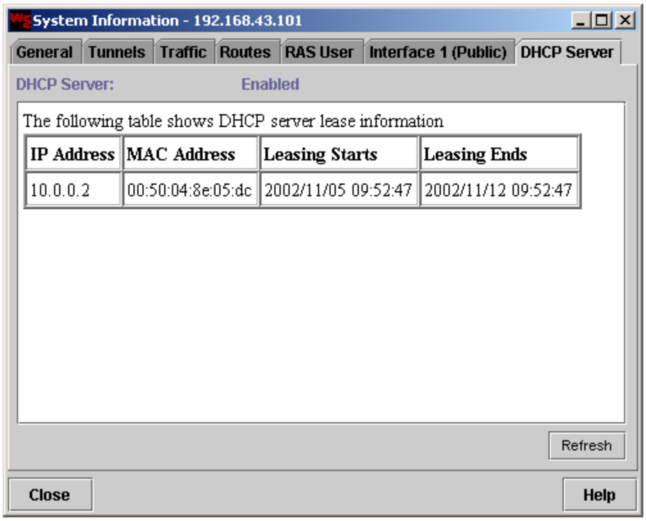
4 When you are finished, click **Close**.

DHCP Server Information

If you have configured the Firebox Vclass appliance to act as a DHCP server, you can use this tab to view the DHCP lease information.

1 From the main Vcontroller page, click **System Information**.
The System Information dialog box appears.

2 Click the **DHCP Server** tab.
THe DHCP server lease information is displayed.



DHCP Server: Enabled

The following table shows DHCP server lease information

IP Address	MAC Address	Leasing Starts	Leasing Ends
10.0.0.2	00:50:04:8e:05:dc	2002/11/05 09:52:47	2002/11/12 09:52:47

3 Click **Refresh** to update the display with the most recent information.

4 When you are finished, click **Close**.

CHAPTER 15

Backing Up and Restoring Configurations

The WatchGuard Vcontroller offers an array of built-in archiving and data restoration capabilities. You can save all your configuration settings and policies in anticipation of a severe data loss, and then reapply that data, when needed, to restore a system.

NOTE

x.509 certificates and software licenses are not archived. You must reimport the original files into an appliance when necessary.

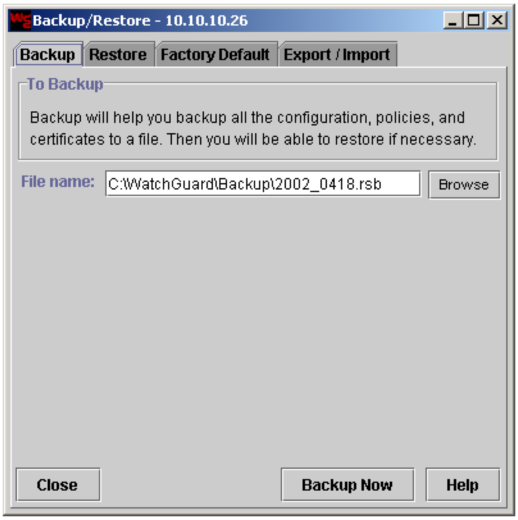
Three scenarios require that you restore your security appliance database:

- The Firebox Vclass appliance crashes and corrupts the current set of configurations and policies.
- A recently modified set of policies is compromised.
- You create and apply a different configuration, and then later want to restore the previous configuration.

Unless you establish a regular schedule of Vcontroller database backups, you risk having to re-create all your configuration entries or policies. Make a habit of keeping regular archive sets available.

Create a Backup File

1 From the main Vcontroller page, click **Back Up/Restore**.
The Backup/Restore dialog box appears.



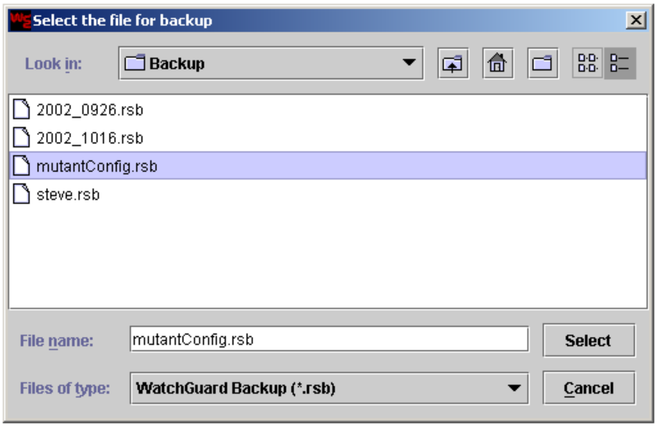
Backup will help you backup all the configuration, policies, and certificates to a file. Then you will be able to restore if necessary.

File name: C:\WatchGuard\Backup\2002_0418.rsb

2 Click the **Backup** tab.

3 To use the default file name and directory, click **Backup Now**.

4 To use a different directory of your choosing, click **Browse**.
The Select Backup File dialog box appears.



Look in: Backup

2002_0926.rsb
2002_1016.rsb
mutantConfig.rsb
steve.rsb

File name: mutantConfig.rsb

Files of type: WatchGuard Backup (*.rsb)

5 Browse to the directory, type a file name of your choosing in the appropriate field, and then click **Select**.
The newly created file path appears in the file name field.

6 Click **Backup Now**.

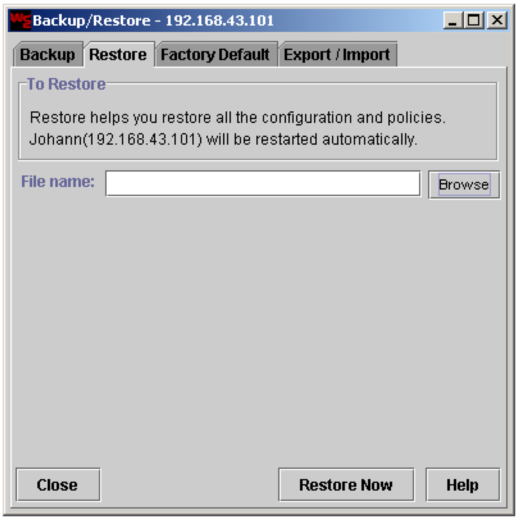
It is strongly recommended that you copy the archived file into a safe location.

Restoring an Archived Configuration

You can restore the Vclass configuration from any previous configuration that you have backed up. Make sure that you are restoring the correct configuration to the appropriate appliance. For example, a backup configuration for a V80 model cannot be used to restore a different Firebox Vclass model.

To restore an archived configuration file:

1 Click the **Restore** tab.



Restore helps you restore all the configuration and policies.
Johann(192.168.43.101) will be restarted automatically.
File name:

2 Click **Browse**.
The Select the file to restore dialog box appears. This dialog box should automatically open to the directory containing all previous archived files.

3 Select the appropriate backup file and then click **Select**.

The backup file name appears in the File Name field.

4 Click **Restore Now**.

A Warning dialog box appears.

5 To restore the appliance, click **OK**; otherwise, click **Cancel**.

After the restoration is complete, another dialog box appears.

6 Click **OK** to proceed.

Another dialog box appears reporting that the server is restarting. This dialog box closes itself when restart is complete.

7 Click the **Log In** button to log into your newly restored Firebox Vclass appliance.

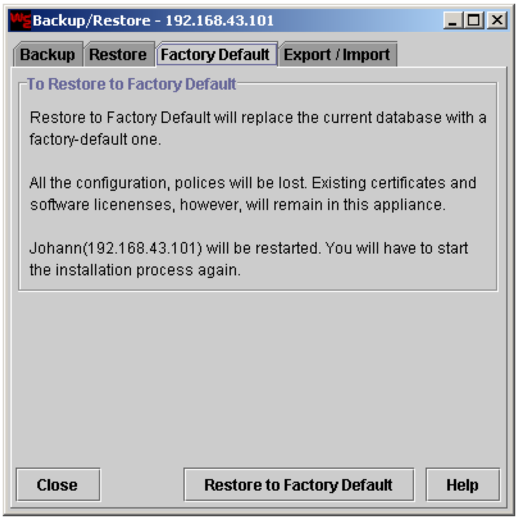
Restoring to the Factory Default

The Vcontroller enables you to revert a Firebox Vclass appliance to the initial factory configuration. This enables you to start over with an appliance as if it just came out of the box.

NOTE

Perform this task only when all other diagnostics or troubleshooting efforts fail.

1 Click the **Factory Default** tab.



Backup/Restore - 192.168.43.101

To Restore to Factory Default

Restore to Factory Default will replace the current database with a factory-default one.

All the configuration, polices will be lost. Existing certificates and software licenenses, however, will remain in this appliance.

Johann(192.168.43.101) will be restarted. You will have to start the installation process again.

2 Read the displayed text. If you want to complete the process, click **Restore to Factory Default**.

A confirmation dialog box appears, asking if you want to erase all the current settings and policies.

3 If you want to continue, click **OK**.

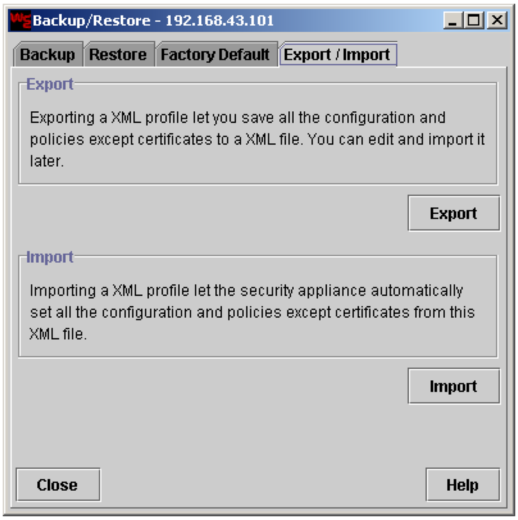
The Firebox Vclass appliance applies the original factory default settings and reboots.

For information on configuring a Firebox Vclass appliance in a factory default state, see "Getting Started" on page 17.

Exporting and Importing Configuration Files

You can export a complete, ready-to-use profile, in XML format, from an active, fully configured Firebox Vclass appliance. You can use this file as an efficient way to store your settings, and later import it to restore your Vclass configuration. After this is done, you may need to make a few adjustments to the file and import any needed CA certificates.

1 Click the **Export/Import** tab.



Export

Exporting a XML profile let you save all the configuration and policies except certificates to a XML file. You can edit and import it later.

Import

Importing a XML profile let the security appliance automatically set all the configuration and policies except certificates from this XML file.

To export an XML file containing the complete configuration settings and policies:

1 Click **Export**.
A Save dialog box appears.

2 Open the destination directory and name the export file.

3 Click **Save**.
When the process is complete, a confirmation dialog box appears.

4 Click **OK**.

To import an XML file containing the complete configuration settings and policies:

1 Click **Import**.
An Open dialog box appears.

2 Locate and select the appropriate file.

3 Click **Open**.
When the process is complete, a confirmation dialog box appears.

4 Click **OK**.
The Firebox Vclass appliance reboots.

Importing a configuration file using Appliance Discovery

Instead of the usual configuration and setup process, you can import a complete appliance profile as part of the device discovery process.

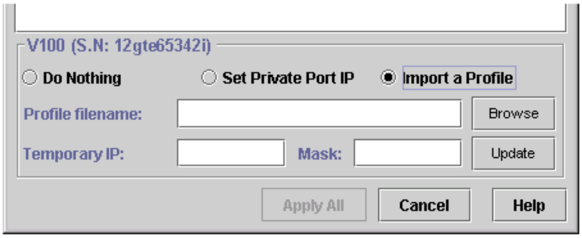
NOTE

No international or high ASCII characters can be extracted and incorporated into the XML file. Only ASCII characters or umbers are permitted in a Firebox Vclass appliance's XML profile.

1 When the **Devices Found** dialog box appears, select the entry of the appliance to configure.

2 Click **Import a Profile**.

Some additional options are displayed in the dialog box, as shown in the following illustration.



V100 (S.N: 12gte65342i)

○ Do Nothing ○ Set Private Port IP ● Import a Profile

3 Click **Browse**.

The Open dialog box appears.

4 Locate and select the XML configuration file you want to apply to this appliance.

Only files with ".xml" extensions are displayed in this dialog box.

5 If needed, in both the Temporary IP and Mask fields, type the appropriate entries. This temporary IP address must be in the same subnet as your administrative workstation.

The Temporary IP and Mask entries are used to configure interface 0 (Private) of the target Vclass appliance so that the XML file can be transferred to that appliance. The entries are temporary because the interface will be reconfigured with the IP address information defined in the XML file after the appliance has been restarted.

6 Click **Update**.

After the profile is imported, the Results dialog box appears.

7 Review the messages and then click **Close**.

8 When the Devices Found dialog box reappears, click **Cancel** to close it.

9 You can now use the Login dialog box to log in to this appliance using the newly assigned IP address.

Editing an exported configuration file

If the exported file is intended for use in other Firebox Vclass appliances, you can make changes to its contents, as described in this section. Because the configuration file is in XML format, you can open it with any text or XML editor to make changes to the contents. After this is done and you have saved the changes, you can then import the configuration file into a Firebox Vclass appliance.

NOTE

Do not attempt to alter or delete the login/TEXT password text. This text is encrypted during the export process. You must use Vcontroller to change your password after the import has been successfully concluded.

The following illustration shows the beginning of a typical configuration file in an XML format.

```
<?xml version="1.0" standalone="yes"?>

<!--DOCTYPE rs-profile SYSTEM "profile.dtd"-->

<profile>

<product-grade>2</product-grade>
<rs-version>1036706512</rs-version>
<using-cpm-profile>0</using-cpm-profile>
<for-version>4.0</for-version>
<for-model>V100</for-model>
<account-list>
<account>
<id>admin</id>
<password>rsyXAP3ZJEP0M</password>
<description>super admin account</description>
<role-list>
<role>super admin</role>
</role-list>
</account>
<account>
<id>admin2k2</id>
```

```
<password>rsgnJUYuNVmbw</password>
<description></description>
<role-list>
<role>admin</role>
</role-list>
</account>
</account-list>
```

The contents are organized within pairs of parameter tags. You can edit included text as required, though you should edit carefully. An erroneous entry can make the appliance unreliable or inoperable.

If the policies include VPN or IPSec policies that rely on automatic IKE exchanges, you must use the **System Configuration** dialog box to initiate a new certificate request process. When the certificate is delivered, import the new certificate into the Vcontroller. Edit the IKE policies to incorporate the new certificate. The IKE exchanges are now enabled.

If you have imported a configuration file into a Firebox Vclass appliance that contains certificates, a default IKE action is automatically inserted into the configuration file. Any IKE policies that refer to the missing certificate will use a default PSK instead.

The default values of the IKE action are as follows:

Name
DEFAULT_PSK

Description
Default PSK-only IKE action

Preshared Key
Default

Mode
Main

PFS
Yes

IKE transform

Authentication
Preshared key

Encryption algorithm
DES

Authentication algorithm
MD5

Lifetime
8 hours

CHAPTER 16

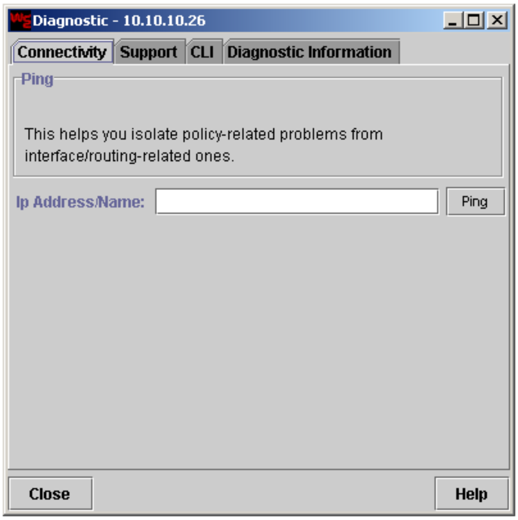
Using the Diagnostics/CLI Feature

This chapter describes a variety of useful troubleshooting features that can help you identify and resolve problems.

Using Connectivity to Test Network Connections

If network connections appear to be broken, you can use the Firebox Vclass appliance to test the hardware and cabling:

1 From the main Vcontroller page, click **Diagnostics/CLI**.
The Diagnostics dialog box appears.



This helps you isolate policy-related problems from interface/routing-related ones.

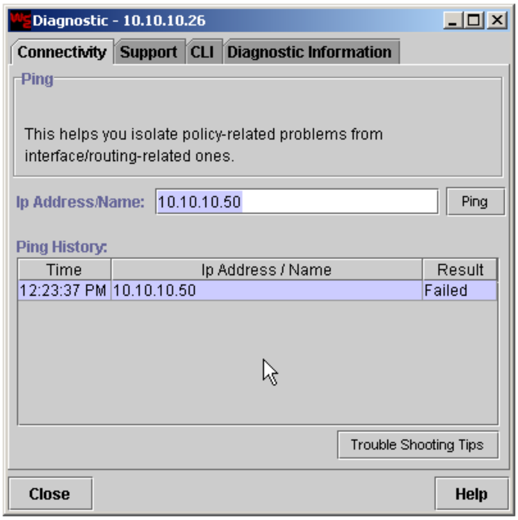
Ip Address/Name:

2 Click the **Connectivity** tab.

3 Type the IP address or DNS host name in the appropriate field.

4 Click **Ping**.

The Ping History table displays the result. This entry describes the time of the test, the address you attempted to ping and the result, either OK or Failed.



This helps you isolate policy-related problems from interface/routing-related ones.

Ip Address/Name: 10.10.10.50

Ping History:

Time	Ip Address / Name	Result
12:23:37 PM	10.10.10.50	Failed

5 If this test has verified that the device is responding to Ping packets from the Firebox Vclass appliance, the physical connection is working.

If this test fails, check all physical connections, cables, hubs, and other hardware components.

NOTE

To obtain WatchGuard Technical Support, visit the WatchGuard Web site at the following URL:
http://www.watchguard.com
For more information on technical support, see "Service and Support" on page 7.

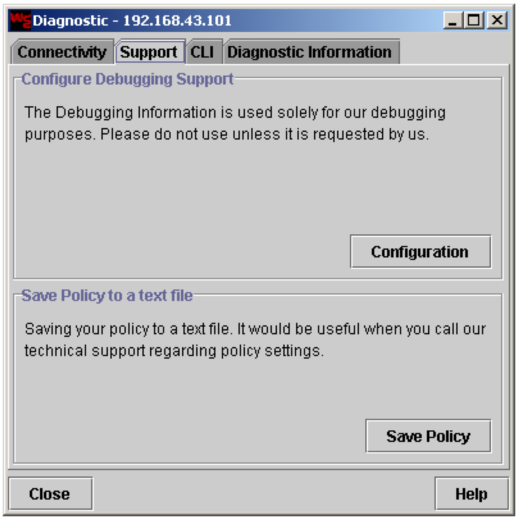
Using the Support Features

The debugging support features are helpful in troubleshooting possible malfunctions, but only in conjunction with technical support. A technical support representative may ask you to use these features and then forward the results to WatchGuard for analysis.

Configuring debugging support

1 From the main Vcontroller page, click **Diagnostics/CLI**.
The Diagnostics dialog box appears.

2 Click the **Support** tab.



Diagnostic - 192.168.43.101

Configure Debugging Support

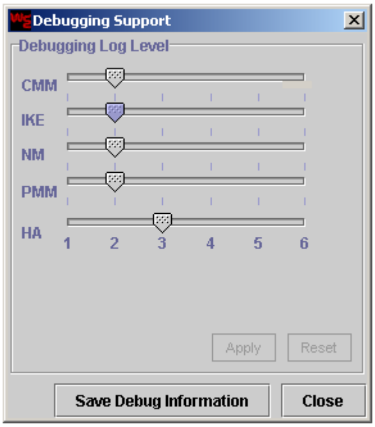
The Debugging Information is used solely for our debugging purposes. Please do not use unless it is requested by us.

Save Policy to a text file

Saving your policy to a text file. It would be useful when you call our technical support regarding policy settings.

3 Click **Configuration**.

The Debugging Support dialog box appears.



Debugging Support

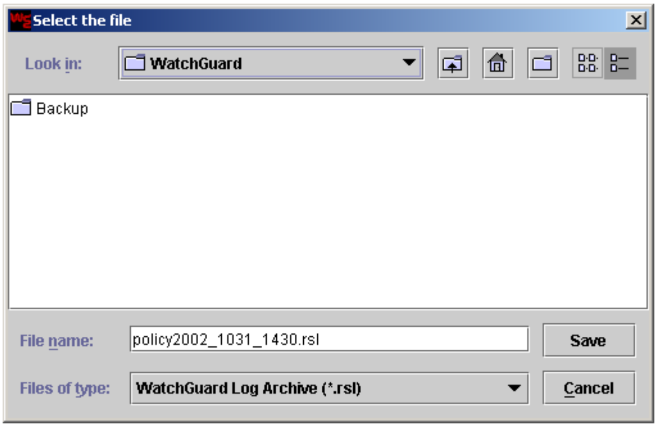
Debugging Log Level

4 Under the direction of technical support, move the sliders to the requested locations.

5 Click **Apply**.

6 Click **Save Debug Information**.

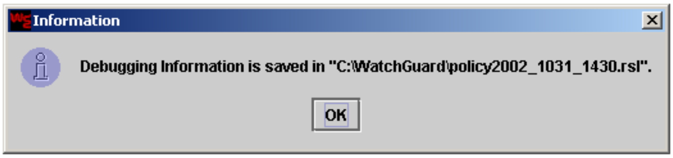
The Select the File dialog box appears.



File name: policy2002_1031_1430.rsl

Files of type: WatchGuard Log Archive (*.rsl)

7 Browse to the proper directory and then click **Save**.
A confirmation dialog box appears.



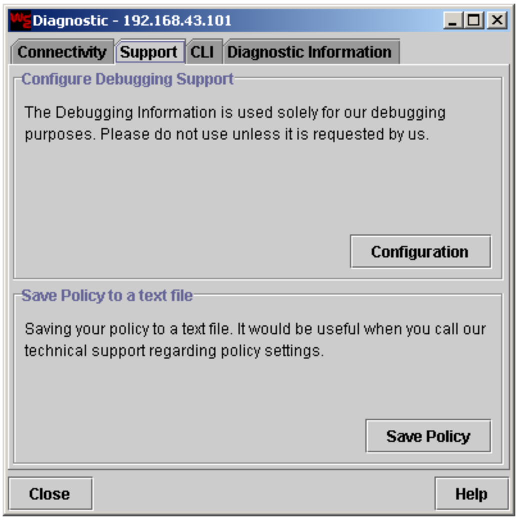
Debugging Information is saved in "C:\WatchGuard\policy2002_1031_1430.rsl".

8 Click **OK**.

Saving a Policy to a text file

1 From the main Vcontroller page, click **Diagnostics/CLI**.
The Diagnostics dialog box appears.

2 Click the **Support** tab.



Configure Debugging Support

The Debugging Information is used solely for our debugging purposes. Please do not use unless it is requested by us.

Save Policy to a text file

Saving your policy to a text file. It would be useful when you call our technical support regarding policy settings.

3 Click **Save Policy**.
The Select the file dialog box appears.

4 Browse to the proper directory and click **Select**.
A confirmation dialog box appears.

5 Click **OK**.

Executing a CLI Script

The CLI (Command Line Interface) feature in Vcontroller can be used to execute an update, maintenance, or other script on your Vclass device.

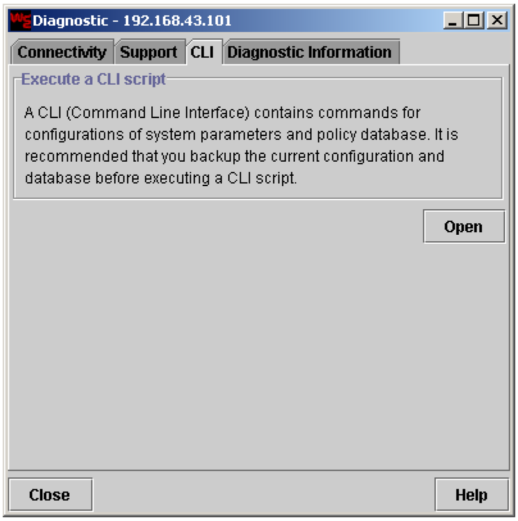
NOTE

This is not an actual command line interface window.

After you have received the script from a network administrator or other personnel and stored it on your file system, you can follow these steps to execute it on your appliance.

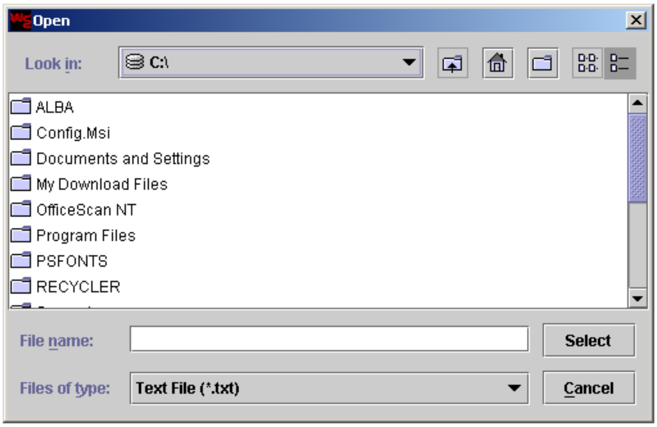
1 From the main Vcontroller page, click **Diagnostics/CLI**.
The Diagnostics dialog box appears.

2 Click the **CLI** tab.



A CLI (Command Line Interface) contains commands for configurations of system parameters and policy database. It is recommended that you backup the current configuration and database before executing a CLI script.

3 Click **Open**.
The Open dialog box appears.



Look in: C:\

ALBA
Config.Msi
Documents and Settings
My Download Files
OfficeScan NT
Program Files
PSFONTS
RECYCLER

Files of type: Text File (*.txt)

4 Browse to the proper directory and select the CLI script.

5 Click **Open** to execute the script.
After the script has been executed, a Confirmation/Restart dialog box appears, informing you that you must now restart the appliance for changes to take effect.

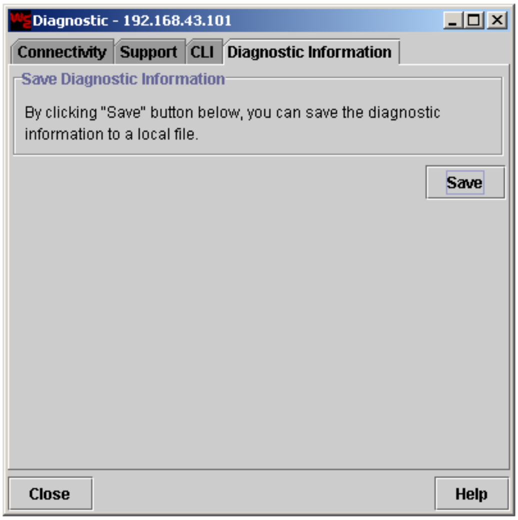
6 Click **OK**.
The appliance reboots.

Saving Diagnostic Information

Saving diagnostic information is helpful in troubleshooting possible malfunctions, but only in conjunction with technical support. A technical support representative may ask you to save diagnostic information and then forward the file to WatchGuard for analysis.

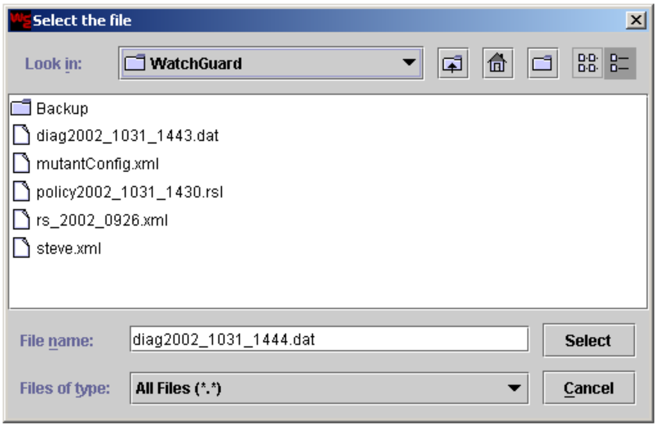
1 From the main Vcontroller page, click **Diagnostics/CLI**.
The Diagnostics dialog box appears.

2 Click the **Diagnostic Information** tab.



By clicking "Save" button below, you can save the diagnostic information to a local file.

3 Click **Save**.
The Save dialog box appears.



File name: diag2002_1031_1444.dat

4 Browse to the proper directory and select the appropriate file.

5 Click **Select**.

A confirmation dialog box appears.

6 Click **OK**.

CHAPTER 17

Setting Up a High Availability System

In a WatchGuard High Availability (HA) system, two Firebox Vclass appliances are connected so that one serves as a ready backup to the other if the main appliance fails while managing network traffic. This chapter guides you in connecting, linking, and running such a high availability (HA) system using two Firebox Vclass appliances in a Primary and Standby relationship.

There are two High Availability modes: Active/Standby and Active/Active. Active/Standby is available for all models that have an HA interface. Active/Active requires the purchase of a software upgrade license, and requires V80 or V100 hardware. Please refer to the WatchGuard Web site for information on purchasing software upgrade licenses:

https://www.watchguard.com/upgrade

Active/Standby

Active/Standby means that when a Primary appliance fails, the passive appliance comes online with a full copy of the state table, to provide maximum uptime and network availability.

Active/Active

The Active/Active option works with two Vclass appliances paired together using redundant High Availability (HA) Ethernet ports. Active/Active uses transparent state failover, which provides a seamless transition if one of the boxes fails and the other must take over. System configuration, policies and firewall, and VPN connections are shared between the two active appliances, so if one fails, the other is fully aware of the state of all connections and can continue carrying the load without dropping any packets.

This chapter discusses High Availability Active/Standby mode. To learn about High Availability Active/Active mode, see the *High Availability Guide* that comes with the license key when you purchase the HA Active/Active upgrade option.

In HA Active/Standby mode, you configure the Standby appliance to mirror the Primary appliance. The Standby appliance will be functionally inactive, waiting for a signal from the Primary that it has failed. If this occurs, the Standby appliance takes over all network management tasks within a very short interval, replacing the failed device.

The WatchGuard High Availability (HA) system is both automatic and transparent. Switching to a backup appliance occurs almost instantaneously.

When active, the Primary appliance regularly sends a “heartbeat” to the standby appliance. If the Primary appliance fails, the heartbeat ceases. When the standby appliance detects three consecutive missed heartbeats, it assumes full network functions and operations within a few seconds.

Prerequisites for a High Availability System

To set up a High Availability Active/Standby system, you need the following:

- Two Firebox Vclass appliances.
- The appliance you use as the Standby appliance must be in the factory default configuration. If you just unpacked this appliance, it is in a factory default state. If the appliance that will be used as the Standby device has already been configured, you must reset it to the factory default configuration using Vcontroller or the Command Line Interface.

Connecting the Appliances

To set up a high availability system, you must connect two Firebox Vclass appliances through the HA port.

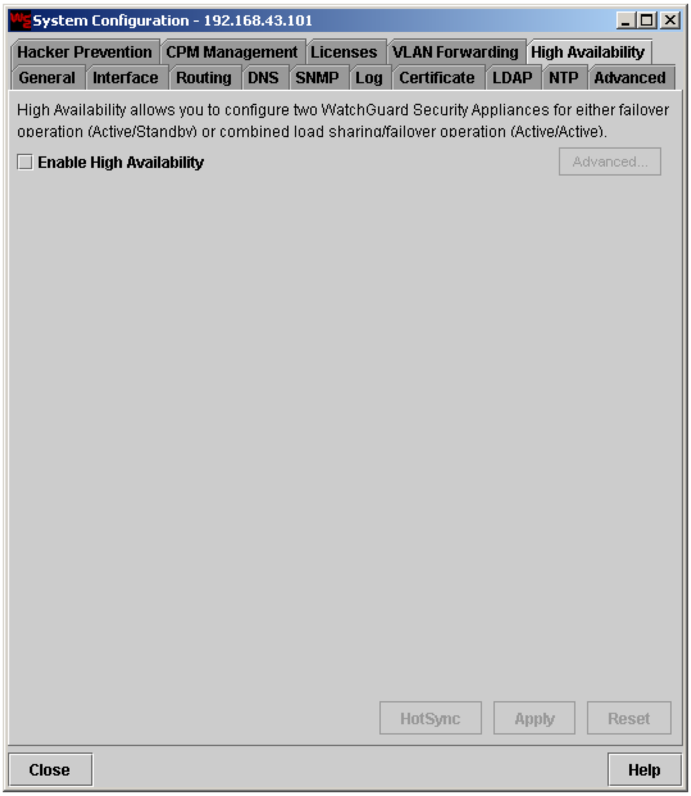
- Connect the Private interface (0) of the Primary appliance to a hub or switch.
- Connect the Private interface (0) of the Standby appliance to the same hub or switch.
- Connect all other interfaces that are being used in the same way. Every interface connection from the Primary appliance to a hub or switch must be matched with a connection from the Standby appliance to the same hub or switch.
- Connect the HA interfaces with crossover cables.
- Connect the Management Station to a hub that is connected to interface 0 (private) on both appliances. The Management Station can also be connected to an HA2 port.

Configuring a Standby Appliance

Use the **High Availability** tab to configure the standby appliance.

1 From the main Vcontroller page, click **System Configuration**.
The System Configuration dialog box appears.

2 Click the **High Availability** tab.
The High Availability settings are displayed.



System Configuration - 192.168.43.101

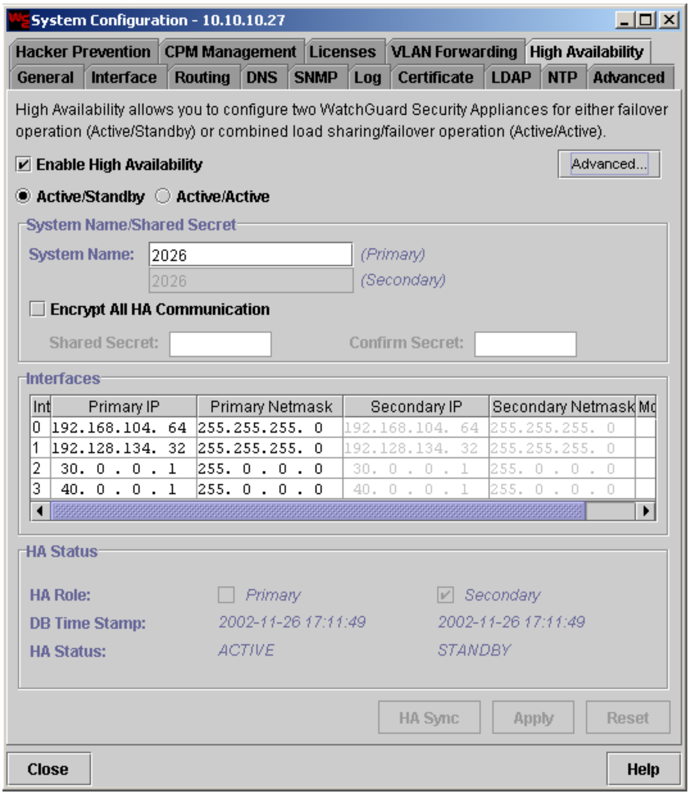
High Availability allows you to configure two WatchGuard Security Appliances for either failover operation (Active/Standby) or combined load sharing/failover operation (Active/Active).

□ Enable High Availability

3 Click the checkbox labeled **Enable High Availability**.

4 Select the **Active/Standby** checkbox.

The following HA options are displayed.



High Availability allows you to configure two WatchGuard Security Appliances for either failover operation (Active/Standby) or combined load sharing/failover operation (Active/Active).

☑ Enable High Availability

● Active/Standby ○ Active/Active

System Name/Shared Secret

System Name: 2026 (Primary)
2026 (Secondary)

□ Encrypt All HA Communication

Shared Secret: Confirm Secret:

Interfaces

Int	Primary IP	Primary Netmask	Secondary IP	Secondary Netmask	Mo
0	192.168.104. 64	255.255.255. 0	192.168.104. 64	255.255.255. 0	
1	192.128.134. 32	255.255.255. 0	192.128.134. 32	255.255.255. 0	
2	30. 0 . 0 . 1	255. 0 . 0 . 0	30. 0 . 0 . 1	255. 0 . 0 . 0	
3	40. 0 . 0 . 1	255. 0 . 0 . 0	40. 0 . 0 . 1	255. 0 . 0 . 0	

HA Status

HA Role:	□ Primary	☑ Secondary
DB Time Stamp:	2002-11-26 17:11:49	2002-11-26 17:11:49
HA Status:	ACTIVE	STANDBY

These default HA settings include the following:

- All of the appliance's interfaces will be monitored. If any interface is detected as "LINK-DOWN," the Secondary appliance will take over.
- The HA heartbeat interval is set to one beat every second.
- The HA Group ID, which uniquely identifies this group (pair) of Firebox Vclass appliances currently backing each other up, is recorded as 3.
- The HA heartbeat is sent through the HA1 interface.
- The appliance you are currently logged into will be configured as the primary.

NOTE

Make sure that the connection links both HA1 ports on the primary and secondary appliances, and that you are using a crossover cable. If the appliance cannot detect the secondary appliance, check the connection and restart the secondary appliance. When this is done, click the Refresh button to redetect the secondary appliance.

5 Type the **System Name** of the Primary appliance in the appropriate field.

6 If desired, click **Encrypt all HA Communication**, and type and confirm a shared secret.

This feature is optional, and can be left blank if you do not need to encrypt information sent between these appliances during normal operation. Encryption is not necessary if the HA1 interfaces are connected directly with a crossover cable.

NOTE

For better performance, leave the HA secret blank. This shared secret is used to encrypt HA state-sync information. VPN tunnel information is always encrypted, even if this encryption is disabled.

7 From the far right of the Interface list, click the **Monitoring** checkboxes to active monitoring on specific interfaces. You may have to scroll the Interfaces list to see this column.

8 To apply the default HA configuration to the Primary appliance, click **Apply**.

9 If you need to perform Advanced configuration tasks, such as setting up HA2 as an HA port, or changing the default primary and standby appliance HA port IP addresses, click **Advanced**. See "Customizing HA System Parameters" on page 289 for more information.

10 Click **HA Sync** to copy the entire configuration and policy database from the Primary appliance to the Standby appliance.

This button is active only if the status indicator in the High Availability tab displays an "OK" message. If this button is not active, make sure that the Standby appliance has been turned on and that all HA interface connections are secure.

A status dialog box appears. When the synchronization is complete, a confirmation dialog box appears. Both appliances are now ready for standby protection.

NOTE

The first time you perform an HA Sync, the standby appliance must be in factory default configuration.

NOTE

Remember to perform HA Sync every time you make any changes to configurations or to the policy database, to assure total operational consistency between Primary and Standby appliances.

Customizing HA System Parameters

You can customize a number of HA parameters using the **Advanced HA Parameters** dialog box. At this level, you can configure the following:

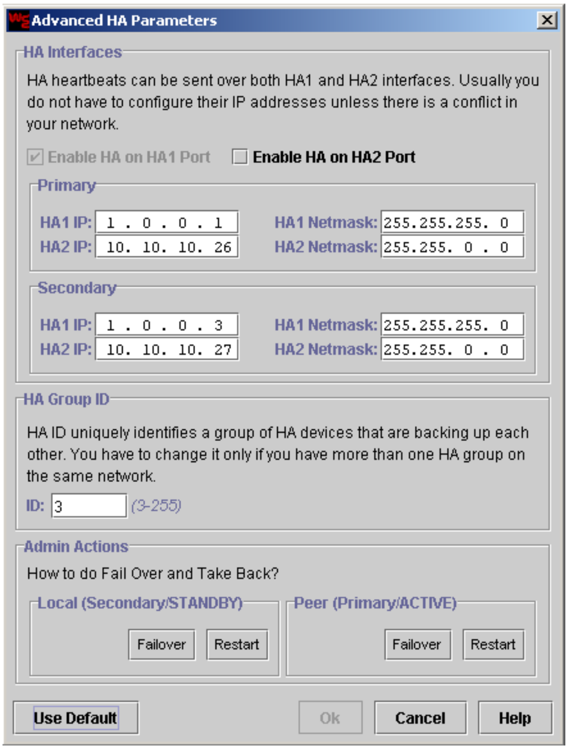
- Send the HA heartbeat to the secondary appliance's HA2 management interface.
- Change the HA group ID.

In addition, you can manually trigger a Failover or Restart event on the Primary or Secondary appliance.

To change any of these settings, follow these steps:

1 Click **Advanced**.

The Advanced HA Parameters dialog box appears.



Advanced HA Parameters

HA Interfaces

HA heartbeats can be sent over both HA1 and HA2 interfaces. Usually you do not have to configure their IP addresses unless there is a conflict in your network.

☑ Enable HA on HA1 Port ☐ Enable HA on HA2 Port

Primary

HA1 IP: 1 . 0 . 0 . 1 HA1 Netmask: 255.255.255. 0

HA2 IP: 10. 10. 10. 26 HA2 Netmask: 255.255. 0 . 0

Secondary

HA1 IP: 1 . 0 . 0 . 3 HA1 Netmask: 255.255.255. 0

HA2 IP: 10. 10. 10. 27 HA2 Netmask: 255.255. 0 . 0

HA Group ID

HA ID uniquely identifies a group of HA devices that are backing up each other. You have to change it only if you have more than one HA group on the same network.

ID: 3 (3-255)

Admin Actions

How to do Fail Over and Take Back?

2 To activate monitoring through the HA ports, click to select the checkbox marked **Enable HA on HA1 Port** and/or **Enable HA on HA2 Port**.

Note that if HA is enabled on the HA2 interface, that interface cannot be used for management access. If you already configured the HA2 interface for management access in the Interface tab of the System Configuration dialog box, reopen that dialog box and undo those entries.

3 If specific IP addresses have been assigned to the HA ports, type the IP addresses and netmasks in each of the two HA Interface fields—Primary and Standby. Otherwise the default addresses are adequate.

You can enter different IP addresses so these ports can be accessed through your local area network.

4 If you plan to set up more than one Primary/Standby system in this subnet, delete the “3” in the **HA Group ID** field and type a number

that uniquely identifies this system within the network context. (The number can range between 3 and 255.)

HA Group IDs are used to identify High Availability Active/Standby pairs on your network. Each HA Active/Standby pair should have a separate Group ID. You need to change this number only if other devices are running the VRRP protocol (using the same VRRP ID) on the networks connected to this appliance. VRRP allows both HA security appliances to share the same MAC and IP addresses.

5 When you have finished, click **OK** to save the parameter entries and close the **Advanced HA Parameters** dialog box.

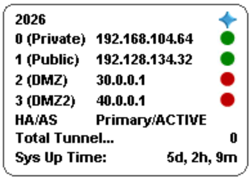
6 When the **High Availability** tab reappears, click **HA Sync** to synchronize your appliances.

7 When you have finished configuring High Availability settings, click **Apply** to apply the settings, or **Reset** to reset the settings.

8 When you have finished, click **Close**.

Checking your HA System Status

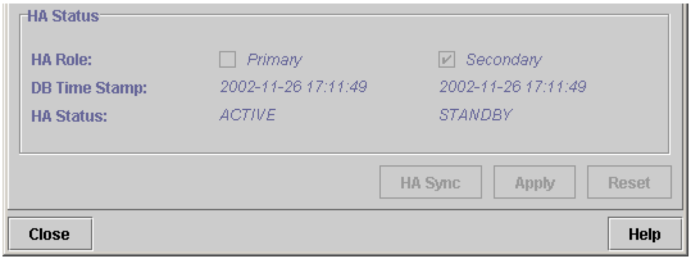
The HA monitor tells you which appliance you are logged into, whether it is Primary or Secondary, and whether it is Active or Failover.



```
2026                                 ✦
0 (Private)   192.168.104.64         🟢
1 (Public)    192.128.134.32         🟢
2 (DMZ)       30.0.0.1               🔴
3 (DMZ2)      40.0.0.1               🔴
HA/AS         Primary/ACTIVE
Total Tunnel...                      0
Sys Up Time:               5d, 2h, 9m
```

Detailed system status

Detailed HA system status is shown in the System Configuration/High Availability dialog box. This status includes the HA role, status, DB timestamp, and failure reason (if one exists) for both systems.



HA Status

HA Role:	□ Primary	☑ Secondary
DB Time Stamp:	2002-11-26 17:11:49	2002-11-26 17:11:49
HA Status:	ACTIVE	STANDBY

To view detailed system status, open the **System Configuration** dialog box and click the **High Availability** tab. You can view the HA status of both the Primary and Standby appliances at the same time. The following list describes the possible Status messages you might see.

Active	The current appliance is active
Standby	The current appliance is standing by
Failed	The current appliance has failed (for example, the link is down)
Takeover	The peer appliance has failed and the current system takes over
Admin	Administration mode
Unavailable	When then current appliance cannot detect its peer appliance, it shows this state in the peer HA status

Additional Preparation for Failover

Make sure, in anticipation of a failover, that you open and edit the existing Event Alarm definition so that you are notified by an SNMP trap, email alert, or both. You should also make sure that all SNMP stations have been registered in the appliances, as can be done in the **System Configuration** dialog box's SNMP tab.

For more information on defining alarms, see "Using Alarm Manager" on page 231.

Index